
Set Up and Maintain Your Salesforce Organization

Salesforce, Spring '24



CONTENTS

Set Up and Maintain Your Salesforce Organization	1
Try Out Salesforce	2
Plan Your Salesforce Rollout	3
Set Up Your Company in Salesforce	5
Manage Your Salesforce Account	359
Manage Users	377
Manage Data Access	472
Import Data Into Salesforce	672
Export Backup Data from Salesforce	722
Back Up Metadata to Protect and Restore Your Customizations	732
Protect Your Data with Salesforce Backup	734
Cache Lightning Platform Data	743
My Domain	747
Protect Your Salesforce Organization	878
Technical Requirements and Performance Best Practices	1212
Monitor Your Organization	1223
Installed Packages	1261
Learn More About Setting Up Salesforce	1283
Index	1285

SET UP AND MAINTAIN YOUR SALESFORCE ORGANIZATION

As a Salesforce administrator—that is, a user assigned to the Administrator profile—you're responsible for setting up your online organization, which means adding users and configuring the system for your needs.

[Try Out Salesforce](#)

Use a trial Salesforce org to evaluate Salesforce before you subscribe. Your trial org includes sample data and various Salesforce features, and you can use it to easily subscribe to Salesforce when you're ready.

[Plan Your Salesforce Rollout](#)

Before you roll up your sleeves and start setting up Salesforce, take a look at the resources available to help you plan your rollout.

[Set Up Your Company in Salesforce](#)

Use the Company Information page in Setup to track what's important about your company's organization in Salesforce. You can also manage your licenses and entitlements. This page contains the information that was provided when your company signed up with Salesforce.

[Manage Your Salesforce Account](#)

Add products and licenses, manage your contracts and renewals, view and download invoices, and get account support right in your org with the Your Account app.

[Manage Users](#)

In Salesforce, each user is uniquely identified with a username, password, and profile. Together with other settings, the profile determines which tasks a user can perform, what data the user can see, and what the user can do with the data.

[Manage Data Access](#)

Salesforce provides a flexible, layered data sharing design that lets admins control user access to data. Managing data access enhances security by exposing only data that's relevant to users. Use permission sets, permission set groups, and profiles to control the objects and fields users can access. Use organization-wide sharing settings, user roles, and sharing rules to specify the individual records that users can view and edit.

[Back Up Metadata to Protect and Restore Your Customizations](#)

Protect your org's customizations, such as custom fields, custom Apex code, page layouts, reports, and permission sets, by backing up your metadata.

[Protect Your Data with Salesforce Backup](#)

Use Salesforce Backup to prevent data loss, recover from data incidents quickly, and simplify your overall data management strategy. Protect your organization from permanent data loss and corruption by automatically generating backups. You can create backup policies for high-value and regulated data, and restore that data in just a few clicks.

[Cache Lightning Platform Data](#)

Using the Platform Cache can enable applications to run faster because they can store reusable data in memory. Applications can quickly access this data, removing the need to duplicate calculations and requests to the database on subsequent transactions.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: All Editions

[My Domain](#)

Showcase your company's brand with a customer-specific subdomain name in your Salesforce org URLs. With My Domain, you can include your company name in your URLs, for example, `https://mycompany.my.salesforce.com`. With these org-specific URLs, you can set up a custom login page, set a custom login policy, offer single sign-on, and allow users to log in with a social account. My Domain also allows you to work in multiple Salesforce orgs in the same browser at the same time.

[Protect Your Salesforce Organization](#)

Salesforce is built from the ground up to protect your data and applications. You can also implement your own security scheme to reflect the structure and needs of your organization. Protecting your data is a joint responsibility between you and Salesforce. The Salesforce security features enable you to empower your users to do their jobs safely and efficiently.

[Technical Requirements and Performance Best Practices](#)

Review the recommended technical requirements and performance best practices to optimize your Salesforce implementation.

[Monitor Your Organization](#)

Salesforce provides a variety of ways to keep tabs on activity in your Salesforce organization so you can make sure you're moving in the right direction.

[Learn More About Setting Up Salesforce](#)

In addition to online help, Salesforce creates guides and tip sheets to help you learn about our features and successfully administer Salesforce.

Try Out Salesforce

Use a trial Salesforce org to evaluate Salesforce before you subscribe. Your trial org includes sample data and various Salesforce features, and you can use it to easily subscribe to Salesforce when you're ready.

As the person who signed up, you become the Salesforce admin. You can add another admins when you add more users.

 **Note:** Features in your trial org depend on the edition that you purchase.

[Start a New Trial](#)

When you sign up for Salesforce, you can choose an industry-specific template with sample data. During your trial period, you can start a new trial with a blank template. To start a new trial abandon your current trial, including all data and customizations. Only usernames are preserved.

[Delete Trial Data](#)

When you sign up for Salesforce, your Salesforce org is initially populated with sample data. During your trial period, Salesforce admins can delete the sample data and all your org's data by using the Delete All Data link.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Professional** and **Enterprise** Editions

Start a New Trial

When you sign up for Salesforce, you can choose an industry-specific template with sample data. During your trial period, you can start a new trial with a blank template. To start a new trial abandon your current trial, including all data and customizations. Only usernames are preserved.

You can start a new trial if you have:

- Fewer than 1,000 rows of data
 - No additional user licenses added by Salesforce
 - No additional functionality enabled by Salesforce
1. From Setup, enter *Start a New Trial* in the **Quick Find** box, then select **Start a New Trial**. This link is available only during your trial period.
 2. Select your language and template preferences.
 3. Enter the requested text stating that you want to abandon your current trial org and all its data, including sample data and data that you've entered.
 4. To confirm that all of your current data will be lost, select the checkbox.
 5. Click **Submit**.
 6. When the confirmation page appears, click **Submit**.

Delete Trial Data

When you sign up for Salesforce, your Salesforce org is initially populated with sample data. During your trial period, Salesforce admins can delete the sample data and all your org's data by using the Delete All Data link.

The Delete All Data link is visible only when all these conditions are met.

- The user has the "Modify All Data" user permission.
 - The org is in a trial state.
 - The org doesn't have portals enabled.
 - The user isn't a Partner Administrator, acting on another user's behalf.
1. From Setup, enter *Delete All Data* in the **Quick Find** box, then select **Delete All Data**.
 2. Enter the requested text stating that you understand that all data in your org will be deleted, including sample data and data that you entered. Your user and admin setup isn't affected.
 3. Click **Submit**.

If data storage limits prevent you from deleting all your trial data this way, use Mass Delete Records to delete your accounts. Then use Delete All Data to delete your remaining trial data. For instructions for using Mass Delete Records, see [Delete Multiple Records and Reports](#) on page 728.

Plan Your Salesforce Rollout

Before you roll up your sleeves and start setting up Salesforce, take a look at the resources available to help you plan your rollout.

If you're wondering how to get started, you might consider working with a consulting partner to take full advantage of the product. Consulting partners are firms that employ Salesforce-certified consultants. Consultants work with you to learn what your company needs,

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

User Permissions Needed

To start a new trial:

- [Modify All Data](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional**, **Essentials**, and **Enterprise** Editions

USER PERMISSIONS

To delete trial data:

- [Modify All Data](#)

design and build your Salesforce organization to meet those needs, and test the organization before you roll it out to your teams. Consulting partners have one goal in mind: Your success with Salesforce.

Rolling out an effective Salesforce organization takes time and thoughtful planning. Working with a partner can help your company harness the power of Salesforce in a way that can be difficult and time-consuming without expert guidance.

Not sure if your company needs expert guidance? Consider how you would respond to the following questions about your company's sales goals.

- Does your company have the internal resources with the time, expertise, and experience to develop the appropriate Salesforce features to solve your business needs?
- Is your company expanding into new business, countries, or industries?
- Do you need a decisive, objective perspective when making business decisions?
- Do you want to see results in weeks, not years?

Still on the fence? Check out this comparison between rolling out Salesforce yourself and rolling out Salesforce with a partner.

Compare	Rolling out Salesforce Yourself	Rolling out Salesforce with a Partner
Qualifications	Sometimes companies have Salesforce-certified employees who can assist with setup.	Consultants are Salesforce-certified.
Experience	Usually employees have little or no Salesforce experience.	Consultants have set up many Salesforce organizations and are knowledgeable about best practices.
Availability of resources for setup	Usually setup competes with your employees' other projects and priorities.	Consultants commit to and deliver on a scope of work for your Salesforce rollout.
External support	Salesforce offers basic support for all Salesforce organizations. Support includes access to self-help (online help articles) and Customer Support agents (guaranteed to respond within 2 days).	Consultants are experienced and well-connected, and can offer personalized support to companies during setup and rollout.
Time commitment	Usually rolling out Salesforce yourself is a significant time commitment unless experienced resources are available.	Usually rolling out Salesforce with a partner is faster, because experienced resources are fully engaged in your project.
Salesforce adoption by your sales teams	When Salesforce isn't rolled out properly, companies run the risk that their sales teams don't recognize the products' value, and don't adopt the product wholeheartedly.	When consultants roll out Salesforce, there is a greater chance that sales teams adopt the product from the start because its value is obvious.
Training resources	Companies are required to customize and roll out their own training plans for employees without mentorship from expert resources.	Salesforce partners can offer experienced mentorship and pre-designed training materials.

To learn more about consulting partners and how to connect with one, check out our website, [Successfully Implement with Salesforce Partners](#).

SEE ALSO:

[Successfully Implement with Salesforce Partners](#)

[Successfully Implement with Salesforce Partners](#)

Set Up Your Company in Salesforce

Use the Company Information page in Setup to track what's important about your company's organization in Salesforce. You can also manage your licenses and entitlements. This page contains the information that was provided when your company signed up with Salesforce.

In sandbox orgs, you can use this page to match provisioned licenses in production to your sandbox organization. The matching process updates your sandbox organization with licenses from production and deletes any licenses in sandbox that aren't in production.

[Manage Information About Your Company](#)

The Company Information page shows all the important information about your company (listed here in alphabetical order). The page also includes the user and feature licenses purchased for your organization.

[Allow the Required Domains](#)

To enable your users to access Salesforce, you must add the standard Salesforce domains to your list of allowed domains.

[Allow Network Access for News, Account Logos, and Automated Account Fields](#)

If your company has policies to restrict certain IP addresses or Salesforce domains, you need to allowlist the following domain and IP addresses before you can use the News, Account Logos, and Automated Account Fields features.

[Web Request Limits](#)

Limits for concurrent usage on web requests.

[Customize the User Interface](#)

Give your users the best working experience you can by setting up the user interface to meet their needs.

[Set Up the Lightning Experience Home Page](#)

Give your users everything they need to manage their day from the Home page in Lightning Experience. Your sales reps can see their quarterly performance summary and get important updates on critical tasks and opportunities. You can also customize the page for different types of users and assign custom pages to different apps and app-and-profile combinations.

[Custom Record Page Settings](#)

Customize the experience users have when working with records in Lightning Experience.

[Language, Locale, and Currency Settings](#)

The Salesforce settings for language, locale, time zone, and currency can affect how objects, such as Accounts, Leads, or Opportunities, are displayed.

[Define Your Fiscal Year](#)

Specify a fiscal year that fits your business needs.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **All** editions

USER PERMISSIONS

To view company information:

- View Setup and Configuration

To change company information:

- Modify All Data

[Einstein Terms and Data Usage](#)

Some Einstein features require you to accept terms and review usage limitations before turning them on. Also, review which data is used for global models.

[Set Up Einstein Search](#)

Find out which objects and fields are searchable. Customize search settings, search result filters, and lookup search. Learn how to improve the search experience for users.

[Provide Maps and Location Services](#)

Maps and location services uses Google Maps to display maps on standard address fields, enables creation of Visualforce maps, and helps users enter new addresses with autocomplete.

[Customize Reports and Dashboards](#)

Set up reports and dashboards to deliver information to your users in the ways that work best for them.

[Release Updates](#)

Salesforce periodically releases updates that improve the performance, security, logic, and usability of your Salesforce org, but that can affect your existing customizations. When these updates become available, Salesforce shows them in the Release Updates node in Setup.

[Organize Data with Divisions](#)

Divisions let you segment your organization's data into logical sections, making searches, reports, and list views more meaningful to users. Divisions are useful for organizations with extremely large amounts of data.

[Salesforce Upgrades and Maintenance](#)

Salesforce reserves up to five minutes of service interruption for major upgrades, but you have access your data during other maintenance events, like splits and migrations.

[Permissions for UI Elements, Records, and Fields](#)

To access UI elements, records or fields in Salesforce requires specific permissions. At a minimum, you must have the "Read" permission to view a tab, record, record field, related list, button, or link. To edit a record or record field, you must have the "Edit" permission.

[Deactivate a Developer Edition Org](#)

When a Developer Edition org has outlived its usefulness and it's time to move on, you can deactivate it or allow it to expire.

[Developer Org Expiration](#)

Developer edition (DE) orgs that haven't been logged into for 180 days are marked as inactive and queued for deletion.

[How Do I Discontinue Service?](#)

If the service doesn't meet your needs, cancel it.

Manage Information About Your Company

The Company Information page shows all the important information about your company (listed here in alphabetical order). The page also includes the user and feature licenses purchased for your organization.

Field	Description
Address	Street address of the organization. Up to 255 characters are allowed in this field.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

The available fields vary according to which Salesforce Edition you have.

Field	Description
Admin Newsletter	Allow administrators in your organization to choose whether they want to receive administrator-targeted promotional emails from Salesforce.
API Requests, Last 24 Hours	The total number of API requests issued by the organization in the last 24 hours. The maximum number of requests depends on your Edition.
City	City in which organization is located. Up to 40 characters are allowed in this field.
Corporate Currency	The currency in which the organization's corporate headquarters reports revenue. Serves as the basis for all currency conversion rates. Only for organizations that use multiple currencies.
Country	Country portion of user's address. Entry is selected from a picklist of standard values, or entered as text. Up to 80 characters are allowed if the field is a text field.
Created By	User who signed up the organization, including creation date and time. (Read only)
Currency Locale	The country or geographic region in which the organization is located. The setting affects the format of currency amounts. For single currency organizations only.
Default Language	<p>The default language that is selected for new users in the organization. This setting determines the language used for the user interface text and help. In all editions except Personal Edition and Database.com, individual users can separately set the language for their own login, which overrides the organization setting. In Group Edition, this field is called <code>Display Language</code>.</p> <p>This setting also determines the language in which all customizations—such as custom fields, tabs, and user interface options—are stored. For customizations, individual users' language settings don't override this setting.</p> <p>If you edit or clone existing filter criteria, check that this setting matches the default language that was configured when the filter criteria was originally set. Otherwise, the filter criteria can be evaluated differently than expected.</p>
Default Locale	The default country or geographic region that is selected for new users in the organization. This setting determines the format of dates, times, and names in Salesforce. In Contact Manager, Group, Professional, Enterprise, Unlimited, Performance, and Developer Edition organizations, individual users can set their personal locale, which overrides the organization setting. In Group Edition, this field is called <code>Locale</code> .

Field	Description
Default Time Zone	Primary time zone in which the organization is located. A user's individual <code>Time Zone</code> setting overrides the organization's <code>Default Time Zone</code> setting. Note: Organizations in Arizona typically select "Mountain Standard Time," and organizations in parts of Indiana that don't follow Daylight Savings Time usually select "Eastern Standard Time."
Division	Group or division that uses the service, for example, PC Sales Group. Up to 40 characters are allowed in this field.
Fax	Fax number. Up to 40 characters are allowed in this field.
Fiscal Year Starts In	If using a standard fiscal year, the starting month and year for the organization's fiscal year. If using a custom fiscal year, the value is "Custom Fiscal Year."
Hide Notices About System Downtime	Select this checkbox to prevent advance notices about planned system downtime from displaying to users when they log in to Salesforce.
Hide Notices About System Maintenance	Select this checkbox to prevent advance notices about planned system maintenance from displaying to users when they log in to Salesforce.
Modified By	User who last changed the company information, including modification date and time. (Read only)
Newsletter	Allow users in your organization to choose whether they want to receive user-targeted promotional emails from Salesforce.
Organization Edition	Edition of the organization, such as Developer Edition or Enterprise Edition.
Organization Name	Name of the organization. Up to 80 characters are allowed in this field.
Phone	Main phone number at organization. Up to 40 characters are allowed in this field.
Primary Contact	Person who is main contact or administrator at the organization. You can enter a name, or select a name from a list of previously defined users. Up to 80 characters are allowed in this field.
Restricted Logins, Current Month	Number of restricted login users who have logged in during the current month. This value resets to zero at the beginning of each month. The maximum number of restricted login users for the organization is in parentheses.
Salesforce Licenses	Number of Salesforce user accounts that can be defined for access to the service. This number represents the Salesforce user licenses for which the organization is billed, if charges apply.

Field	Description
Salesforce Organization ID	Code that uniquely identifies your organization to Salesforce.
State/Province	State or province portion of user's address. Entry is selected from a picklist of standard values, or entered as text. Up to 80 characters are allowed if the field is a text field.
Streaming API Events, Last 24 Hours	The total number of Streaming API events used by the organization in the last 24 hours. The maximum number of events depends on your edition.
Zip	Zip or postal code of the organization. Up to 20 characters are allowed in this field.
Used Data Space	Amount of data storage in use. The value is expressed as a measurement (for example, 500 MB) and as a percentage of the total amount of data storage available (for example, 10%).
Used File Space	Amount of file storage in use. The value is expressed as a measurement (for example, 500 MB) and as a percentage of the total amount of file storage available (for example, 10%).

SEE ALSO:

[Set Up Your Company in Salesforce](#)

Allow the Required Domains

To enable your users to access Salesforce, you must add the standard Salesforce domains to your list of allowed domains.

If your users have general access to the Internet, no action is required.

If you control your users' or servers' access to the Internet through allowlists, add these domains to ensure that you receive all Salesforce content.

Salesforce Domains to Allow

To enable all Salesforce functionality, add these Salesforce-managed domains.

Domain	Use
*.bluetail.salesforce.com	News, account logos, and automated account fields.
*.documentforce.com	Content (files) stored in Salesforce orgs without enhanced domains. If enhanced domains are deployed, this domain isn't necessary.
*.force.com	Visualforce pages, Lightning pages, and content (files) stored in Salesforce. If enhanced domains aren't enabled, this domain is also used for Experience Cloud sites and Salesforce Sites.
*.forceusercontent.com	User content stored in Salesforce orgs without enhanced domains. If enhanced domains are deployed, this domain isn't necessary.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: All Editions.

Domain	Use
*.force-user-content.com	User content stored in Salesforce.
*.lightning.com	Lightning container components in orgs without enhanced domains. If enhanced domains are deployed, this domain isn't necessary.
*.salesforce.com	Salesforce login authentication, plus setup for Sales, Service, and Experience Cloud. Also used for multiple Salesforce content sites, including Salesforce Help, Salesforce Developers, Salesforce Admins, Trailblazer Communities, and Trailhead.
*.salesforceliveagent.com	Chat, Omni-Channel, and SOS
*.salesforce-communities.com	Experience Builder for Experience Cloud sites in orgs without enhanced domains. If enhanced domains are deployed, this domain isn't necessary.
*.salesforce-experience.com	Experience Builder for Experience Cloud sites.
*.salesforce-hub.com	Customer 360 Data Manager
*.salesforce-scrn.com	Next generation Omni-Channel engagement (examples: voice and messaging)
*.salesforce-setup.com	Setup pages in Salesforce.
*.salesforce-sites.com	Salesforce Sites.
*.site.com	Experience Cloud sites.
*.sfdcopens.com	Email tracking.
trailblazer.me	Sign-up, login, and profile and settings management with multiple Salesforce-related sites, including AppExchange, IdeaExchange, Salesforce Help, Trailhead, and Trailblazer Communities.
*.trailhead.com	Enablement Sites (myTrailhead).
*.visualforce.com	Visualforce pages in orgs without enhanced domains. If enhanced domains are deployed, this domain isn't necessary.

Domains to Allow for the Salesforce Mobile App

To ensure that you receive all content in the Salesforce mobile app, add these domains.

- analytics.localytics.com
- manifest.localytics.com

Domains to Allow for Login Screen Content

These domains are used to deliver content in the right frame of your login screen. If you don't allow these domains, the right side of a non-customized login page can display page-load errors.

- *.sfdcstatic.com
- secure.eloqua.com
- *.google.com

- *.doubleclick.net
- www.facebook.com
- *.google-analytics.com

The right frame content is displayed in the following URLs.

- login.salesforce.com
- test.salesforce.com
- <yourInstance>.salesforce.com
- A My Domain URL without a customized login page (for example, norms.my.salesforce.com)

Domains to Allow for Trailblazer Identity Login Screen Content

These domains are used to deliver content in the Trailblazer Identity login screen. If you don't allow these domains, you'll see a blank screen when trying to log in via Trailblazer Identity.

- *.oktacdn.com
- *.okta.com
- *.lightningdesignsystem.com
- *.sfdcstatic.com
- cdn.cookieclaw.org
- *.onetrust.com
- *.googletagmanager.com
- *.google-analytics.com

Allow Network Access for News, Account Logos, and Automated Account Fields

If your company has policies to restrict certain IP addresses or Salesforce domains, you need to allowlist the following domain and IP addresses before you can use the News, Account Logos, and Automated Account Fields features.

The News, Automated Account Fields, and Account Logos features are scheduled for retirement in Winter '24 on October 13, 2023.

1. Allowlist the domain *.bluetail.salesforce.com.
2. Allowlist the following IP addresses.

34.224.144.232	52.21.43.255	34.215.243.17
34.197.49.208	52.54.5.76	54.191.9.66
52.44.146.48	54.236.191.28	52.88.106.13
34.225.107.166	52.21.109.221	54.187.26.178
34.206.188.121	107.23.62.176	52.42.8.120
54.210.4.174	107.23.102.197	54.218.71.194
54.208.220.233	54.87.200.56	35.161.196.219

EDITIONS

News, Account Logos, and Automated Account Fields are available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited** Editions

52.73.79.3	52.86.60.223	54.187.245.205
52.22.254.22	34.200.157.195	52.10.193.59
34.193.204.122	52.205.154.40	35.160.155.237
52.4.158.80	52.54.242.233	34.212.90.52
52.3.73.106	54.175.157.145	52.27.222.241
34.205.234.140	34.195.58.231	34.210.120.217
107.23.108.83	34.196.109.221	34.213.118.122
54.82.148.169	52.22.224.140	54.200.63.165
52.4.238.209	52.72.252.194	54.186.66.113
107.21.49.246	52.203.119.68	54.148.190.73
34.200.8.4	107.23.29.15	34.208.143.103

Web Request Limits

Limits for concurrent usage on web requests.

To ensure that resources are available for all Salesforce users, limits are placed on the number of long-running Web requests that one organization can send at the same time. Salesforce monitors the number of concurrent requests issued by all users logged in to your org and compares that number against the maximum limit. In this way, the number of concurrent requests is kept below the maximum limit. The limit ensures that resources are available uniformly to all orgs and prevents deliberate or accidental over-consumption by any one org.

If too many requests are issued by users in your org, you might have to wait until one of them has finished before you can perform your task. For example, assume that MyCorporation has 100,000 users. At 9:00 AM, each user requests a report that contains 200,000 records. Salesforce starts to run the report for all users until the maximum number of concurrent requests has been met. At that point, Salesforce refuses to take any additional requests until some of the reports have completed.

Similar limits are placed on requests issued from the API.

Customize the User Interface

Give your users the best working experience you can by setting up the user interface to meet their needs.

From Setup, search for *User Interface* in the *Quick Find* box.

[User Interface Settings](#)

Modify your org's user interface by enabling or disabling these settings.

[Set Up the User Interface in Salesforce Classic](#)

The improved Setup user interface provides a streamlined experience for viewing and managing personal and administrative setup tasks.

[Disable the Salesforce Notification Banner](#)

User Interface Settings

Modify your org's user interface by enabling or disabling these settings.

User Interface Settings

Setting	Description
Enable Collapsible Sections	Collapsible sections let users collapse or expand sections on their record detail pages by using the arrow icon next to the section heading. When enabling collapsible sections, verify that your section headings are displayed for each page layout. Sections remain expanded or collapsed until the user changes the settings for that tab. If your org has enabled record types, Salesforce remembers a different setting for each record type.
Show Quick Create	The Quick Create area on a tab home page allows users to create a record quickly with minimal information. It displays by default on the tab home pages for leads, accounts, contacts, and opportunities. You can control whether the Quick Create area is displayed on all relevant tab home pages. The Show Quick Create setting also affects whether users can create records from within the lookup dialog. Creating records in the lookup dialog is available only if Quick Create is available for your chosen record type. In addition, users always need the appropriate "Create" permission to use Quick Create even though it displays for all users.
Enable Hover Details	Hover detail displays an interactive overlay containing record details. Details appear when users hover over a link to that record in the Recent Items list on the sidebar, or in a lookup field on a record detail page. Users

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

The available user interface settings vary according to which Salesforce Edition you have.

USER PERMISSIONS

To modify user interface settings:

- [Customize Application](#)

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

The user interface settings vary according to which Salesforce edition you have.

USER PERMISSIONS

To modify user interface settings:

- [Customize Application](#)

Setting	Description
	<p>can quickly view information about a record before clicking to view or edit the record. The record's mini page layout determines which fields are included in the hover details. Users can't customize which fields appear. This option is enabled by default.</p> <p>To view hover details for a record, users need the appropriate sharing access, and field-level security access for the fields in the mini page layout.</p>
Enable Related List Hover Links	<p>Related list hover links display at the top of record detail pages and custom object detail pages in Setup. Users can hover over a related list link to display the list and its number of records in an interactive overlay. Users quickly view and manage the related list items from the overlay. Users can also click a related list hover link to jump to the related list without having to scroll down the page. This option is enabled by default.</p>
Enable Separate Loading of Related Lists	<p>When enabled, users see primary record details immediately. As the related list data loads, users see a progress indicator. Separate loading can improve performance on record detail pages for orgs with large numbers of related lists. This option applies only to Salesforce Classic and is disabled by default. The options for separately loading related lists don't apply to Visualforce pages, the Self-Service portal, or other pages for which you can't control the layout.</p>
Enable Separate Loading of Related Lists of External Objects	<p>When enabled, related lists of external objects are loaded separately from primary record details and related lists of standard and custom objects. External objects behave similarly to custom objects, except that they map to data that's stored outside your Salesforce org. It can take a while to retrieve data from an external system, depending on the network latency and availability of the external system. This option applies only to Salesforce Classic and is enabled by default. The options for separately loading related lists don't apply to Visualforce pages, the Self-Service portal, or other pages for which you can't control the layout.</p>
Enable Inline Editing	<p>Inline editing lets users quickly edit field values, right on a record's detail page. This option is enabled by default and applies to all users in your org.</p> <p>To enable enhanced lists for profiles in particular, select Enhanced Profile List Views in User Management Settings.</p>
Enable Enhanced Lists	<p>Enhanced lists give you the ability to quickly view, customize, and edit list data to speed up your daily productivity. When enabled with the <code>Enable Inline Editing</code> setting, users can also edit records directly from the list, without navigating away from the page. This option is enabled by default.</p> <p>To enable enhanced lists for profiles in particular, Enable Enhanced Profile List Views available in User Management Settings.</p>
Enable the Salesforce Classic 2010 User Interface Theme	<p>This option isn't related to Lightning Experience. In this case, "Salesforce Classic" refers to the newer version of Salesforce Classic, which is the interface that immediately precedes Lightning Experience. Enabling this option turns on the updated Salesforce Classic look and feel. Disabling it turns on the Salesforce Classic 2005 user interface theme —the <i>classic, classic</i> Salesforce interface.</p> <p>Some features, like Chatter, require the Salesforce Classic 2010 user interface theme. Disabling this theme automatically disables Chatter in both Salesforce Classic and Lightning Experience.</p> <p>Only users with supported browsers see the Salesforce Classic.</p> <p>Salesforce Classic isn't supported in portals or on the Console tab.</p>

Setting	Description
Disable Navigation Bar Personalization in Lightning Experience	When selected, users can't add or reorder the items included in the navigation bar for any app. However, Salesforce recommends disabling navigation personalization per app instead. From Setup in Lightning Experience, go to the App Manager . For the desired app, select App Options . Select Disable end user personalization of nav items in this app . This option applies only to Lightning Experience.
Clear Workspace Tabs for Each New Console Session	When selected, previously open workspace tabs aren't loaded in new console sessions. From Setup in Lightning Experience, go to the App Manager , select the console app that you want, and then select App Options . Select Clear workspace tabs for each new console session . This option applies only to Lightning Experience and is disabled by default. Workspace tabs are restored when the browser page is refreshed, even when this option is enabled. But in Safari pages, workspace tabs aren't restored upon refresh. When this option is enabled, opening a new console session clears pinned and unpinned tabs.
Enable Tab Bar Organizer	The Tab Bar Organizer arranges tabs in the main tab bar to prevent horizontal scrolling of the page. The Organizer dynamically determines how many tabs can display based on the width of the browser window. It puts tabs that extend beyond the browser's viewable area into a dropdown list. <ul style="list-style-type: none"> • The Tab Bar Organizer isn't available with the partner portal or Customer Portal. • The Tab Bar Organizer is only available with the Salesforce Classic. Orgs using the Salesforce Classic can enable the feature, but it isn't available to users until the newer theme is also enabled. • The Tab Bar Organizer isn't available on Internet Explorer 6.
Enable Printable List Views	Printable list views let users easily print list views. If it's enabled, users click the Printable View link from any list view to open a new browser window, displaying the list view in a print-ready format. The link is located next to the Help for this Page link in the colored title bar of the page.
Enable Spell Checker on Tasks and Events	Available in all editions. Enables the Check Spelling button when users create or edit tasks or events. The spell checker analyzes the Description field on events and the Comments field on tasks.
Enable Customization of Chatter User Profile Pages	Enables administrators to customize the tabs on the Chatter user profile page. This includes adding custom tabs or removing default tabs. If disabled, users see the Feed and Overview tabs only.
Change Default Display Density Setting in Lightning Experience	This option isn't related to Salesforce Classic, Experience Builder sites, or the Salesforce mobile apps. The display density controls field label alignment and the amount of space between page elements. Decide what the default is for your org on the Density Settings setup page. Users can choose their own display density at any time. You can't override a user's display density setting. Depending on which edition of Salesforce you have, your org's default display setting varies. Two settings are available. The Comfy setting places the labels on the top of fields and has more space between page elements. Compact is a denser view with labels to the left of fields and less space between page elements.
Disable Lightning Experience Transition Admin Reminders	Salesforce displays a reminder every 45 days to admins (users with Modify All Data and Customize Application user permissions) working in Salesforce Classic with the countdown to the auto-activation of the Turn on Lightning Experience critical update. The reminder continues repeating until the admin turns on Lightning Experience or the update auto-activates. Salesforce also displays a series of suggested actions to admins in orgs where Lightning Experience isn't turned on to help prepare orgs for when the Turn on Lightning Experience Critical Update is activated. When this setting is selected,

Setting	Description
	the countdown reminder and the series of recommended actions don't appear for any of the org's admins.
Enable ICU formats for en_CA locale	After enabling ICU language and locale formats through a critical update, this setting also enables them for the English (Canada) locale.

Sidebar Settings

Setting	Description
Enable Collapsible Sidebar	<p>The collapsible sidebar enables users to show or hide the sidebar on every page that normally includes it. When enabled, the collapsible sidebar is available to all users in your org, but each user can choose how to display the sidebar. Users can leave the sidebar visible, or they can collapse it and show it only when needed by clicking the edge of the collapsed sidebar.</p> <p>Call center users don't see incoming calls if they collapse the sidebar.</p> <p>If your org uses divisions, we recommend that you keep the sidebar pinned and visible so you always have access to the Divisions dropdown list.</p>
Show Custom Sidebar Components on All Pages	<p>If you have custom home page layouts that include components in the sidebar, this option makes the sidebar components available on all pages for all org users. If you only want certain users to view sidebar components on all pages, grant those users the "Show Custom Sidebar On All Pages" permission.</p> <p>If the Show Custom Sidebar Components on All Pages user interface setting is selected, the Show Custom Sidebar On All Pages permission is not available.</p>

Calendar Settings

Setting	Description
Enable Home Page Hover Links for Events	<p>This option affects only Salesforce Classic. Enables hover links in the calendar section of the Home tab. On the Home tab, users can hover the mouse over the subject of an event to see the details of the event in an interactive overlay. This option is enabled by default. This checkbox only controls the Home tab; hover links are always available on other calendar views.</p> <p>The fields available in the event detail and edit overlays are defined in a mini page layout.</p> <p>If you create all day events, we recommend adding the All Day Event field to the events mini page layout.</p>
Enable Drag-and-Drop Editing on Calendar Views	<p>This option affects only Salesforce Classic. You can't disable drag-and-drop in Lightning Experience. Enables dragging of events on single-user, daily and weekly calendar views. Dragging allows users to reschedule events without leaving the page. This option is enabled by default.</p> <p>Calendar views can load less quickly when this checkbox is enabled.</p>

Setting	Description
Enable Click-and-Create Events on Calendar Views	This option affects only Salesforce Classic. Lets users create events on day and weekly calendar views by double-clicking a specific time slot and entering event details in an interactive overlay. The fields available in the event detail and edit overlays are defined in a mini page layout. Recurring events and multi-person events aren't supported for click-and-create events on calendar views.
Enable Drag-and-Drop Scheduling on List Views	This option affects only Salesforce Classic. Lets users create events associated with records by dragging records from list views to weekly calendar views and entering event details in an interactive overlay. This option is disabled by default. The fields available in the event detail and edit overlays are defined in a mini page layout.
Enable Hover Links for My Tasks List	This option affects only Salesforce Classic. Enables hover links for tasks in the My Tasks section of the Home tab and on the calendar day view. This option is enabled by default. Users can hover the mouse over the subject of a task to see the details of that task in an interactive overlay. Your administrator can configure the information presented on these overlays.
Enable Japanese Imperial Calendar for the Japanese Locale	This option affects Lightning Experience and the Salesforce mobile app. Enables the Japanese imperial calendar for users who use the Japanese locale.

Setup Settings

Setting	Description
Enable Enhanced Page Layout Editor	When enabled, the enhanced page layout editor replaces the current interface for editing page layouts with a feature-rich WYSIWYG editor that includes several improvements.
Enable Streaming API	Enables Streaming API, which lets you receive notifications for changes to data that match a SOQL query that you define in a secure and scalable way. This field is selected by default. If your Salesforce edition has API access and you don't see this checkbox, contact Salesforce.
Enable Dynamic Streaming Channel Creation	Enables dynamic channel creation when using the generic streaming feature of Streaming API. When enabled, generic streaming channels get dynamically created when clients subscribe, if the channel hasn't already been created. This field is selected by default. If your Salesforce edition has API access and you don't see the checkbox, contact Salesforce.
Enable "Delete from Field History" and "Delete from Field History Archive" User Permissions	Enables the user permissions that allow you to delete field history and field history archive records. This field isn't selected by default.
Enable Custom Object Truncate	Enables truncating custom objects, which permanently removes all the records from a custom object while keeping the object and its metadata intact for future use.
Enable Improved Setup User Interface	When disabled, users with Salesforce Classic access their personal settings from the Setup menu. When enabled, users with Salesforce Classic access their personal settings from the My Settings menu, accessible from the username menu. The Setup link is also moved from the username menu to the App Menu. If you change this setting, be sure to notify all users in your org.

Setting	Description
Enable Advanced Setup Search (Beta)	<p>When enabled, users can search for Setup pages, custom profiles, permission sets, public groups, roles, and users from the sidebar in Setup. When disabled, users can search for Setup pages only.</p> <ul style="list-style-type: none"> Advanced Setup Search is in beta; it's production quality but has known limitations. Some searchable items (such as permission sets) aren't available in some editions. Users can't search for items that aren't included in their edition.
Use custom address fields	<p>When enabled, the Address custom field type is available in Object Manager. For more information, see Custom Address Fields in Salesforce Help.</p> <p>Before you enable custom address fields, review these important considerations.</p> <ul style="list-style-type: none"> This feature can't be disabled. This feature has limitations. For details, see Custom Address Fields Requirements and Limitations in Salesforce Help.

Advanced Settings

Setting	Description
Activate Extended Mail Merge	<p>Enables Extended Mail Merge for your org. When selected, the Mass Mail Merge link is available in the Tools area on the home pages for accounts, contacts, and leads. Also, single mail merges requested from the Activity History related list on a record are performed using Extended Mail Merge functionality.</p> <p>Before users create mail merge documents using Extended Mail Merge, admins must set up the feature. First, from Setup, in the Quick Find box, enter <i>User Interface</i>, and then select User Interface. Under the Advanced section, select Enable Extended Mail Merge. Admins can indicate whether they want all users' mail merge documents to be saved to Salesforce Documents, or only documents over 3 MB. After the feature is enabled, admins must create mail merge templates in Microsoft® Word, and upload mail merge templates to Salesforce.</p>
Always save Extended Mail Merge documents to the Documents tab	<p>Mail merge documents generated using Extended Mail Merge are added to the user's documents folder on the Documents tab, rather than delivered as email attachments. Users are sent confirmation emails when their mail merge requests have completed. Those emails include links for retrieving generated documents from the Documents tab. These documents count against your org's storage limits.</p>

Set Up the User Interface in Salesforce Classic

The improved Setup user interface provides a streamlined experience for viewing and managing personal and administrative setup tasks.

When the improved Setup user interface is enabled in an organization, you see several differences from the original user interface.

- The Setup menu is accessed from the Setup link on the upper-right corner of any Salesforce page.
- The Setup menu is organized into goal-based categories: Administer, Build, Deploy, Monitor, and Checkout.
- Personal settings, which all Salesforce users can edit, are available from a separate My Settings menu.

To access My Settings, click your name in the upper-right corner of any Salesforce page, then click **My Settings**. You can also access My Settings from your Chatter profile page: in the right pane, click **My Settings**.

- The My Settings home page includes quick links for easily accessing the most commonly used personal settings tools and tasks.

 **Important:** When enabled, the improved Setup user interface is activated for every user in an organization. Be sure to notify your organization before enabling or disabling this setting.

To enable the improved Setup user interface, from Setup, enter *User Interface* in the **Quick Find** box, then select **User Interface**, then select **Enable Improved Setup User Interface**.

 **Note:** The improved Setup user interface:

- Is not supported in Internet Explorer version 6
- Is available only when the new user interface theme is enabled

[Find Items in Setup with Advanced Setup Search \(Beta\)](#)

With Advanced Setup Search, users can search for many types of items in Setup. These items including approval items, custom objects and fields, custom profiles, permission sets, workflow items, users, and so on.

[Setup Search Results Page \(Beta\)](#)

The Setup Search Results page displays various types of items in Setup that match your search terms, including approval items, custom objects and fields, custom profiles, permission sets, workflow items, users, and so on.

EDITIONS

Available in: Salesforce Classic

Available in: **All** editions except **Database.com**

Find Items in Setup with Advanced Setup Search (Beta)

With Advanced Setup Search, users can search for many types of items in Setup. These items including approval items, custom objects and fields, custom profiles, permission sets, workflow items, users, and so on.

 **Note:** Advanced Setup Search is in beta. It is production quality but has known limitations.

To use Advanced Setup Search, verify that the Advanced Setup Search user interface setting is enabled. From Setup, enter *User Interface* in the **Quick Find** box, then select **User Interface**, then scroll to **Enable Advanced Setup Search (Beta)**. If Advanced Setup Search is disabled, the Setup search box returns the titles of pages in the Setup menu, but not individual items that you created or edited in Setup.

Advanced Setup Search is multipurpose, allowing you to use it in different ways.

- To find Setup pages, type part or all of a Setup page name in the Setup Search box. As you type in this box, you immediately see Setup pages whose names match what you're typing. Click the name of the page to open it.
- To find Setup records or objects, enter at least two consecutive characters of the item you want and click  or press Enter. In the Setup Search Results page that appears, select the item you want from the list.

 **Note:** Some searchable items (such as permission sets) aren't available in some editions. Users can't search for items that aren't included in their edition.

 **Example:** For example, let's say you want to see all the installed packages in your organization. Enter *inst*. As you enter letters, the Setup menu shrinks to include only the menus and pages that match your search terms. You quickly see the link for the page you want (**Installed Packages**).

Next, perhaps you want to change the password for one of your users, Jane Smith. Enter *smi t* and click . From the Setup Search Results page, click the Jane Smith result to go directly to her user detail page.

Setup Search Results Page (Beta)

The Setup Search Results page displays various types of items in Setup that match your search terms, including approval items, custom objects and fields, custom profiles, permission sets, workflow items, users, and so on.

 **Note:** Advanced Setup Search is in beta. It is production quality but has known limitations.

In the Setup Search Results page the left pane shows each category with the number of results in parentheses.

- Click any category to see only that category's results.
- If you've filtered your results by category, click **All Results** to show all search results.
- Click a result name to open it or click **Edit**.
- Use the search box at the top of the page to search Setup again.

Search terms that match a user's name or Experience Cloud site nickname (the `Nickname` field in the user detail page) return results that show the user's name only. If the nickname doesn't match the username, the result might not be obvious. For example, if a user who's named Margaret Smith has the nickname Peggy, a search for *peg* returns Margaret Smith.

EDITIONS

Available in: both Salesforce Classic (**not available in all orgs**) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To enable Advanced Setup Search:

- **Customize Application**

To search Setup:

- **View Setup and Configuration**

EDITIONS

Available in: Salesforce Classic (**not available in all orgs**)

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

 **Tip:** When viewing setup search results, bookmark the results page in your Web browser to easily perform the same search in the future. For example, if you often search for "smit", you can bookmark the results page to perform the same search again. The URL for this bookmark would be something like

`https://MyCompany.salesforce.com/ui/setup/SetupSearchResultsPage?setupSearch=smit.`

SEE ALSO:

[Find Items in Setup with Advanced Setup Search \(Beta\)](#)

Set Up the Lightning Experience Home Page

Give your users everything they need to manage their day from the Home page in Lightning Experience. Your sales reps can see their quarterly performance summary and get important updates on critical tasks and opportunities. You can also customize the page for different types of users and assign custom pages to different apps and app-and-profile combinations.

- From Setup, enter *Lightning App Builder* in the **Quick Find** box, then select **Lightning App Builder**. Click **New** to create a Lightning Home page, or click **Edit** next to an existing Home page.
- While editing a Lightning app, select the **Pages** tab, then click **New Page** or **Open Page**.
- While viewing a Home page, click  and select **Edit Page** to create an editable copy of the current Home page.

[Set a New Default Home Page](#)

Set a new default Home page to surface the information that's most relevant for your users. All users see the default Home page unless they have profiles that are assigned to another Home page.

[Assign Custom Home Pages to Specific Apps and Profiles](#)

Assign home pages to different apps and app-and-profile combinations to give your users access to a Home page perfect for their role.

[Lightning Experience Home Permissions and Settings](#)

Give your users access to opportunity details and other permissions so they can get the most out of the Home page.

EDITIONS

Available in: Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

Set a New Default Home Page

Set a new default Home page to surface the information that's most relevant for your users. All users see the default Home page unless they have profiles that are assigned to another Home page.

You can set the default Home page in these ways.

- From Setup, enter *Lightning App Builder* in the **Quick Find** box, then select **Lightning App Builder**.
After you save a page, click **Activate** from the Page Saved dialog, or click **Activation** and select **Set this page as the default Home page**.
- While editing a Lightning app, select the **Pages** tab, click **Open Page**, then click **Activation** and select **Set this page as the default Home page**.
- In Setup—Enter *Home* in the **Quick Find** box, then select **Home**.
Click **Set Default Page** and select a page. To restore the standard Home page, select **System Default**.

Assign Custom Home Pages to Specific Apps and Profiles

Assign home pages to different apps and app-and-profile combinations to give your users access to a Home page perfect for their role.

You can set page assignments by app in three different ways. You can use the Lightning App Builder to assign profiles to a single Home page, but Setup offers more control over page assignments.

-  **Note:** This applies only to Lightning apps. Classic apps can be viewed in Lightning Experience, but you can't display different Home pages assigned for specific apps and profiles. Upgrade Classic apps to Lightning apps in the App Manager to take advantage of Lightning Experience features.
- From Setup, enter *Lightning App Builder* in the **Quick Find** box, then select **Lightning App Builder**.
After you save a page, click **Activate** from the Page Saved dialog, or click **Activation**.
- While editing a Lightning app, select the **Pages** tab, click **Open Page**, then click **Activation**.
- In Setup—Enter *Home* in the **Quick Find** box, then select **Home**.

EDITIONS

Available in: Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

USER PERMISSIONS

To create and save Lightning Pages in the Lightning App Builder

- Customize Application

To view Lightning Pages in the Lightning App Builder

- View Setup and Configuration

EDITIONS

Available in: Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

USER PERMISSIONS

To create and save Lightning Pages in the Lightning App Builder

- Customize Application

To view Lightning Pages in the Lightning App Builder

- View Setup and Configuration

Lightning Experience Home Permissions and Settings

Give your users access to opportunity details and other permissions so they can get the most out of the Home page.

For information about adding news to the Home page, see “Account Settings” in the Salesforce Help.

Today’s Events shows the next five meetings scheduled today. Today’s Tasks shows the next five tasks due today.

The performance chart and Key Deals display opportunity information about a rep’s sales team if they have an associated team. Otherwise, the chart displays opportunities owned by the rep. The performance chart isn’t compatible with custom fiscal years. If you have custom fiscal years enabled in your org, create your own reports and dashboards to display on the Home page.

To populate the performance chart, Key Deals, and the Assistant, users must have these permissions.

Table 1: Required Permissions for Home Features

Permission or Setting	Performance Chart	Key Deals	Assistant
Read access to the Opportunity object and sharing access to relevant opportunities			
Read access to the Opportunity object’s Amount field			
Read access to the Opportunity object’s Probability field			
“Run Reports” user permission enabled for users			
Closed opportunities or open opportunities with a probability over 70% during the current fiscal quarter			
Read access to the Lead object			

For information about configuring action buttons in the Assistant, see “View Important Updates with the Assistant” in the Salesforce Help.

Custom Record Page Settings

Customize the experience users have when working with records in Lightning Experience.

[Lightning Experience Record Page Views](#)

Choose the default view for record pages in Lightning Experience. There are two out-of-the-box options, each with a different focus and organization. Pick the view that supports your users’ business needs and preferences.

[Set the Default Lightning Experience Record Page View](#)

Pick the default view for record pages in Lightning Experience. A record view determines how record information is organized and presented to users.

EDITIONS

Available in: Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

EDITIONS

Available in: Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

[Activities View](#)

Choose a default for how activities display on record pages in Lightning Experience. The views focus on different information and behave differently. Users can change their view preference in their personal settings.

[Set the Default Activities View](#)

You can set the default view for how users work with activities. Users can change their view preference in their personal settings.

Lightning Experience Record Page Views

Choose the default view for record pages in Lightning Experience. There are two out-of-the-box options, each with a different focus and organization. Pick the view that supports your users' business needs and preferences.

Full View

Displays record information in a data-dense, single column. This view emphasizes details and related lists by putting all the information on the same page. If you're transitioning to Lightning Experience, this view is similar to Salesforce Classic.

 **Important:** To maintain performance quality, Full view isn't available for all org configurations. To access Full view your page layout must have:

- No more than 50 fields
- No more than 12 related lists
- No inline Visualforce components

EDITIONS

Available in: Lightning Experience and the Salesforce mobile app for iOS and Android

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Opportunity Information

Opportunity Owner	Steve Service	Close Date	10/30/2018
Opportunity Name	Advanced Productions Corp* - 130K	Stage	Needs Analysis
Account Name	Advanced Interconnections Corp	Probability (%)	75%
Type	Existing Business	Amount	\$150,000.00
Summary	Advanced Productions Corp* - 130K, Follow up in 2 weeks to assess opportunity		
Reason Lost			

Open Activities (10)

	SUBJECT	NAME	TASK	DUE DATE	ASSIGNED TO	LAST MODIFIED DATE/...
1	Meeting with ACME Industries Headquarters		<input checked="" type="checkbox"/>	3/6/2019	Carol White	3/6/2019 11:13 AM
2	April 4th Amer. Sales Monthly Meeting		<input checked="" type="checkbox"/>	3/6/2019	Carol White	3/6/2019 11:12 AM
3	Monthly sync up with Ed	Ed Flachbarth	<input type="checkbox"/>	2/26/2019	Carol White	2/21/2019 5:30 PM
4	Call to Art for follow up		<input type="checkbox"/>	2/25/2019	Carol White	2/21/2019 5:25 PM
5	Follow up email		<input checked="" type="checkbox"/>	2/21/2019	Carol White	2/21/2019 5:27 PM
6	Send over comps		<input checked="" type="checkbox"/>	2/19/2019	Carol White	2/21/2019 5:24 PM
7	Internal Call regarding Advanced Productions		<input checked="" type="checkbox"/>	2/12/2019	Carol White	2/21/2019 5:30 PM
8	Call with Internal Sales Leads		<input checked="" type="checkbox"/>	1/30/2019	Carol White	2/21/2019 5:30 PM
9	Quartley Sales Kick-off		<input checked="" type="checkbox"/>	1/16/2019	Carol White	2/21/2019 5:30 PM
10	Monthly Sales Report to HQ		<input checked="" type="checkbox"/>	1/2/2019	Carol White	2/21/2019 5:29 PM

Activity History (8)

	SUBJECT	NAME	RELATED TO	DUE DATE	ASSIGNED...	LAST MODIFIED DA...
1	Email: Let team up on this contract		Burlington Textiles Weaving Plant Generator	9/13/2018	Carol White	9/13/2018 10:38 AM

Note: You can't collapse sections on the record detail page on the Salesforce mobile app.

Grouped View

Groups record information across tabs and columns. This view helps users focus on what's needed in the moment, and minimizes scrolling.

The screenshot shows a Salesforce record page for an Opportunity. At the top, there is a navigation bar with 'Sales' selected and a search bar. Below the navigation bar, the record title 'Opportunity Burlington Textiles Weaving Plant Generators' is displayed, along with action buttons: '+ Follow', 'New Case', 'Submit for Approval', and 'Change Owner'. Key fields include Account Name (Burlington Textiles Corp of America), Close Date (11/13/2019), Amount (\$375,000.00), Opportunity Owner (Admin User), and Probability (85%).

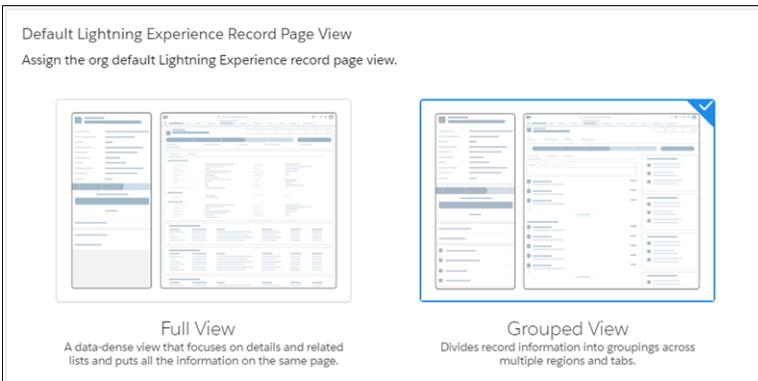
A progress bar shows the opportunity's stages: Proposal/P... (active), Negotiatio..., and Closed. A 'Mark Stage as Complete' button is visible. The main content area is divided into 'Activity' and 'Chatter' tabs. The 'Activity' tab is active, showing a 'Compose' button and a list of activities. The 'Next Steps' section includes a task 'April 4th Amer. Sales Monthly Meeting' due on Apr 5. The 'Past Activities' section lists several tasks and events, such as 'Loop in Jim to support contract' (Oct 15) and 'Meeting - European Sales Leads on Grow...' (12:00 AM | Yesterday).

On the right side, there are two panels. The 'Contact Roles (3)' panel lists: Josh Davis (Economic Buyer, Director, Warehouse Mgmt), Sean Forbes (Evaluator, CFO), and Andy Young (Business User, SVP, Operations). The 'Stage History (3+)' panel shows a history of three stages, all at the 'Proposal/Price Quote' stage, with details on amount, probability, expected revenue, close date, and last modified date.

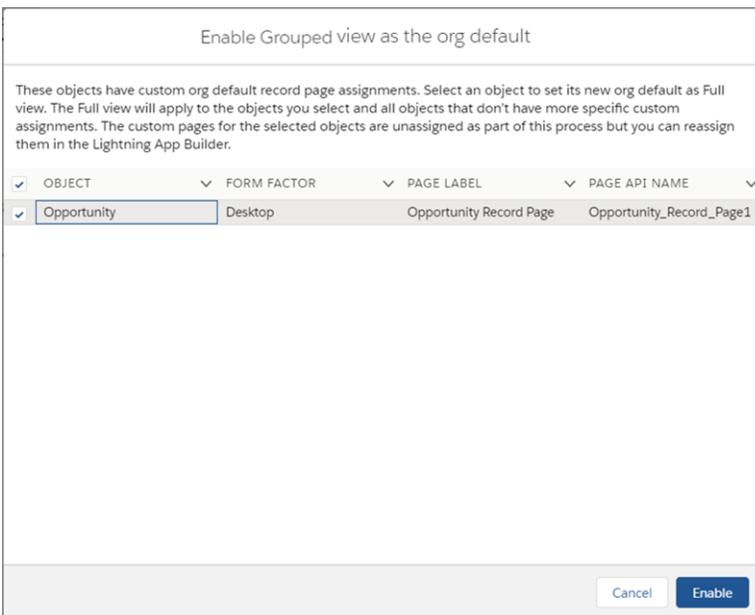
Set the Default Lightning Experience Record Page View

Pick the default view for record pages in Lightning Experience. A record view determines how record information is organized and presented to users.

1. In Setup, enter *Record Page Settings* in the Quick Find box, and select **Record Page Settings**.
2. Select the default Lightning Experience record page view.



3. Click **Save**.
If objects have a custom default record page assignment, a window appears listing them.



4. Click **Enable**.

The new view applies to the objects you select and all objects that don't have specific custom assignments. The custom pages for the selected objects are unassigned as part of this process but you can reassign them in the Lightning App Builder.

EDITIONS

Available in: Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

USER PERMISSIONS

To set the Lightning Record Page View:

- Customize Application

 **Note:** If your record page doesn't show the view you select, refresh the page.

You can assign Full view or Grouped view to specific apps, record types, or profiles by creating a new Lightning page and cloning it from the desired view.

Activities View

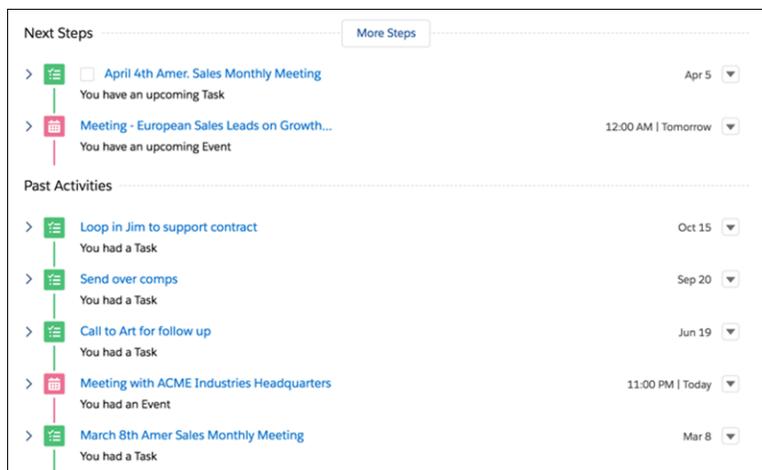
Choose a default for how activities display on record pages in Lightning Experience. The views focus on different information and behave differently. Users can change their view preference in their personal settings.

The activity timeline view shows details for each task, event, and email in an expandable timeline view.

EDITIONS

Available in: Lightning Experience and the Salesforce mobile app for iOS and Android

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions



Section	Activity Type	Title	Description	Date
Next Steps	Task	April 4th Amer. Sales Monthly Meeting	You have an upcoming Task	Apr 5
	Event	Meeting - European Sales Leads on Growth...	You have an upcoming Event	12:00 AM Tomorrow
Past Activities	Task	Loop in Jim to support contract	You had a Task	Oct 15
	Task	Send over comps	You had a Task	Sep 20
	Task	Call to Art for follow up	You had a Task	Jun 19
	Event	Meeting with ACME Industries Headquarters	You had an Event	11:00 PM Today
	Task	March 8th Amer Sales Monthly Meeting	You had a Task	Mar 8

The related lists view shows details for each task, event, and email in the Open Activities and Activity History related lists.

Open Activities (10)
6 Items - Sorted by Due Date - Updated a few seconds ago

	SUBJECT	NAME	TASK	DUE DATE	ASSIGNED TO	LAST MODIFIED DATE/...
1	Meeting with ACME Industries Headquarters		<input checked="" type="checkbox"/>	3/6/2019	Carol White	3/6/2019 11:13 AM
2	April 4th Amer. Sales Monthly Meeting		<input checked="" type="checkbox"/>	3/6/2019	Carol White	3/6/2019 11:12 AM
3	Monthly sync up with Ed	Ed Flachbarth	<input checked="" type="checkbox"/>	2/26/2019	Carol White	2/21/2019 5:30 PM
4	Call to Art for follow up		<input type="checkbox"/>	2/25/2019	Carol White	2/21/2019 5:25 PM
5	Follow up email		<input checked="" type="checkbox"/>	2/21/2019	Carol White	2/21/2019 5:27 PM
6	Send over comps		<input checked="" type="checkbox"/>	2/19/2019	Carol White	2/21/2019 5:24 PM
7	Internal Call regarding Advanced Productions		<input checked="" type="checkbox"/>	2/12/2019	Carol White	2/21/2019 5:30 PM
8	Call with Internal Sales Leads		<input checked="" type="checkbox"/>	1/30/2019	Carol White	2/21/2019 5:30 PM
9	Quarterly Sales Kick-off		<input checked="" type="checkbox"/>	1/16/2019	Carol White	2/21/2019 5:30 PM
10	Monthly Sales Report to HQ		<input checked="" type="checkbox"/>	1/2/2019	Carol White	2/21/2019 5:29 PM

[View All](#)

Activity History (8)
4 Items - Sorted by Last Modified Date - Updated a few seconds ago

	SUBJECT	NAME	RELATED TO	DUE DATE	ASSIGNED TO	LAST MODIFIED DA...
1	Email: Let team up on this contract		Burlington Textiles Weaving Plant Generator	9/13/2018	Carol White	9/13/2018 10:38 AM
2	Email: Meeting on 11/04/18		Burlington Textiles Weaving Plant Generator	9/13/2018	Carol White	9/13/2018 10:36 AM
3	Email: Follow up email		Burlington Textiles Weaving Plant Generator	9/13/2018	Carol White	9/13/2018 10:32 AM
4	Review contract with Client		Burlington Textiles Weaving Plant Generator	9/13/2018	Carol White	9/13/2018 10:37 AM

All standard Lightning Experience record pages support both views.

Set the Default Activities View

You can set the default view for how users work with activities. Users can change their view preference in their personal settings.

1. In Setup, enter *Record Page Settings* in the Quick Find box, and select **Record Page Settings**.
2. Select the default activities view for your org.

Default Activities View (desktop only)

Choose the default way users work with activities on record pages. Users can change this preference in their user settings. [Tell Me More](#)



Related Lists
Give users a view of their activities with the Open Activities and Activity History related lists.



Activity Timeline
Give users a timeline view where they can manage their current and past activities.

i If Einstein Activity Capture is enabled, the Activity Timeline option is required.

If Einstein Activity Capture is enabled, the Activity Timeline option is required.

3. Click **Save**.

If your record page doesn't immediately show the view you select, refresh the page. For custom Lightning pages, make sure that the relevant component for the activity view is present.

EDITIONS

Available in: Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To set the Activities View:

- Customize Application

Language, Locale, and Currency Settings

The Salesforce settings for language, locale, time zone, and currency can affect how objects, such as Accounts, Leads, or Opportunities, are displayed.

In a single currency organization, Salesforce administrators set the currency locale, default language, default locale, and default time zone for their organizations. Users can set their individual language, locale, and time zone on their personal settings pages.

In a multiple currency organization, Salesforce administrators set the corporate currency, default language, default locale, and default time zone for their organizations. Users can set their individual currency, language, locale, and time zone on their personal settings pages. For unauthenticated guest users, date and time formats on Salesforce Sites are based on the user's browser settings instead of the user's personal locale.

 **Note:** Single language organizations cannot change their language, although they can change their locale.

EDITIONS

Available in: Lightning Experience and Salesforce Classic ([not available in all orgs](#))

Available in: **Group, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

Setting	Who can edit the setting
Currency	User in a multiple currency organization
Corporate Currency	Administrator in a multiple currency organization
Currency Locale	Administrator in a single currency organization
Default Currency ISO Code	Not editable
Default Language	Administrator
Default Locale	Administrator
Default Time Zone	Administrator
Information Currency	Not editable
Language	User
Locale	User
Time Zone	User

Administrator Settings

Administrators can edit these language settings:

- Language Preferences—Select the displayed languages for this org.
- Default Language—This Company Information setting applies to all new users until they select their personal language. This setting also determines the language in which all customizations—such as custom fields, tabs, and user interface options—are stored. For customizations, users' personal language settings don't override this default setting. Some setup items that are manually entered by an administrator can be translated in the Translation Workbench.

Administrators can change this setting by editing the company information.

The Salesforce web user interface, Salesforce for Outlook, Connect Offline, and Connect for Office are available in multiple languages.

User Settings

Users can choose a personal language from the languages that the administrator selected for the org. All on-screen text, images, buttons, and Salesforce Help display in this language.

Text entered by users remains in the language in which it was entered.

[Select Languages for Your Org](#)

Choose the languages available to your users.

[Locales Overview](#)

Locales determine the display formats for date and time, users' names, addresses, and commas and periods in numbers. The start day of the week for calendars varies per locale. For single-currency organizations, locales also set the default currency for the organization when you select them in the `Currency Locale` picklist on the Company Information page.

[Set Your Personal or Organization-Wide Currency](#)

If you have a single-currency organization, you can set the default currency for your organization. Multi-currency organizations don't have a default currency. Instead, change your corporate currency or your personal currency.

[Edit Conversion Rates](#)

You can manage static exchange rates between your active and inactive currencies and the corporate currency by editing the conversion rates. These exchange rates apply to all currency fields used in your organization. In addition to these conversion rates, some organizations use dated exchange rates for opportunities and opportunity products.

[Supported Time Zones](#)

You can find a list of Salesforce supported time zones and codes for your organization under your personal settings.

[Local Name Fields](#)

Local name fields are additional standard text fields that allow you to define original or translated text for certain fields on Account, Contact, and Lead objects. For example, you can define local name fields for a contact so that their name appears in a language appropriate for their locale.

[Enable the Japanese Imperial Calendar](#)

Display the imperial calendar for users with the Japanese (Japan) locale.

Select Languages for Your Org

Choose the languages available to your users.

1. From Setup, select **Language Settings**.
2. If you wish to enable end-user languages, check **Enable end-user languages**. All end-user languages are populated into the Available Languages list.

 **Note:** Unchecking **Enable end-user languages** unchecks **Enable platform-only languages** and removes all end-user languages and platform-only languages from the Available Languages and Displayed Languages list. You can't uncheck this option if any end-user language or platform-only language is your org's default language or in use by any user.

While end-user languages display within the Salesforce application, Help and Setup are not translated into these languages.

3. If you wish to enable platform-only languages, check **Enable platform-only languages**. All platform-only languages are populated into the Available Languages list.

 **Note:** Unchecking **Enable platform-only languages** removes all platform-only languages from the Available Languages and Displayed Languages list. You can't uncheck this option if any user is currently using a platform-only language or you selected a platform-only language as your org's default language.

No default translation is provided for platform-only languages.

4. To make a language available to your end users, select the language in the Available Languages list. Click the right arrow under **Add**. The language is added to the Displayed Language list.
5. To make a language unavailable to your end users, select the language in the Displayed Language list. Click the left arrow above **Remove**.

 **Note:** Displayed languages that appear in gray are currently used by your company, users, or both. They cannot be removed.

6. Click **Save**.

Locales Overview

Locales determine the display formats for date and time, users' names, addresses, and commas and periods in numbers. The start day of the week for calendars varies per locale. For single-currency organizations, locales also set the default currency for the organization when you select them in the `Currency Locale` picklist on the Company Information page.

 **Note:** For unauthenticated guest users, date and time formats on Salesforce Sites are based on the user's browser settings instead of the user's personal locale.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions** except **Database.com**

USER PERMISSIONS

To view Language Settings:

- View Setup and Configuration

To change Language Settings:

- Customize Application

EDITIONS

Available in: Lightning Experience and Salesforce Classic ([not available in all orgs](#))

Available in: **Group, Professional, Enterprise, Performance, Unlimited, Database.com**, and **Developer** Editions

[Go Global with New International Locale Formats](#)

To keep the Salesforce Platform up to date with the latest international standards, we adopted a new set of locale formats in Winter '20. Locales control the formats for dates, times, currencies, addresses, names, and numeric values. We currently use International Components for Unicode (ICU) version 71.1, which uses the Unicode Common Locale Data Repository (CLDR) version 41. By default, orgs created before Winter '20 use the locale formats provided by Oracle's Java Development Kit (JDK). This update will be enforced on a rolling basis starting in Spring '24, but you can adopt them now.

[Salesforce Supported Locales and ICU Formats](#)

Salesforce supported locales and their corresponding International Components for Unicode (ICU) formats for name, address, numbers, currencies, dates, and times. We use ICU version 71.1, which uses the Unicode Common Locale Data Repository (CLDR) version 41. These formats are available upon activation of the Enable ICU Formats critical update and require version 45.0 or later of the Salesforce platform API.

[Salesforce Supported Locales and JDK Formats](#)

Salesforce supported locales and their corresponding Oracle's Java Development Kit (JDK) formats for name, address, numbers, currencies, dates, and times. We use JDK version 11, which uses Common Locale Data Repository (CLDR) version 33. We replace these formats with the International Components for Unicode (ICU) formats in Spring '24. Or, now you can adopt the new formats through the Enable ICU Formats release update.

SEE ALSO:

[Autocomplete Addresses](#)

Go Global with New International Locale Formats

To keep the Salesforce Platform up to date with the latest international standards, we adopted a new set of locale formats in Winter '20. Locales control the formats for dates, times, currencies, addresses, names, and numeric values. We currently use International Components for Unicode (ICU) version 71.1, which uses the Unicode Common Locale Data Repository (CLDR) version 41. By default, orgs created before Winter '20 use the locale formats provided by Oracle's Java Development Kit (JDK). This update will be enforced on a rolling basis starting in Spring '24, but you can adopt them now.

The new locale formats are available with version 45.0 and later of the Salesforce platform API.

EDITIONS

Available in: both Salesforce Classic (**not available in all orgs**) and Lightning Experience

Available in: all editions

[Adopt the ICU Locale Formats](#)

To keep your org up to date, review the high-level process to successfully migrate to the new International Components for Unicode (ICU) locale formats. Some of the formats differ from the ones provided by Oracle's Java Development Kit (JDK). Understand how to determine the impact of changes on your org, and learn about the updates required to support the new formats.

[Determine Whether Your Org Uses ICU or JDK Locale Formats](#)

To prepare for the move to the International Components for Unicode (ICU) library from Oracle's Java Development Kit (JDK) library, whether ICU is enabled in your org, or whether you're using JDK and must adopt the ICU locale formats. ICU is the new standard and enforced through a release update.

[Considerations for Adopting the ICU Locale Formats](#)

Learn why Salesforce chose to adopt the International Components for Unicode (ICU) locale formats. Understand why we recommend testing the new formats in a sandbox and enabling them in production before they're enforced. Then review recommendations on handling installed packages, custom code, and notifying your users.

Determine the Locales in Use

To identify the locales used in your org, you can use an SQL query, a report, or both. When locale formats change, your adoption effort depends on the locales used in your org. For example, when you migrate from Oracle's Java Development Kit (JDK) locale formats to International Components for Unicode (ICU) locale formats, or when existing locale formats change.

Identify Changes to Your Locales with ICU

To ensure that you understand the impact of migrating from Oracle's Java Development Kit (JDK) locale formats to International Components for Unicode (ICU) locale formats, determine the specific locale format changes.

Differences Between JDK and ICU Locale Formats

Here are all the differences between Oracle's Java Development Kit (JDK) locale formats and the International Components for Unicode (ICU) locale formats. The changes are listed by locale or platform-only language. By default, orgs created before Winter '20 use the locale formats provided by Oracle's JDK. ICU locale formats replace the JDK formats in Salesforce for all orgs in Spring '24, but you can adopt them now.

Enable the ICU Locale Formats

To test the International Components for Unicode (ICU) locale formats before they're enforced in Spring '24, enable a test run in the Enable ICU Locale Formats release update. Then enable the formats for the English (Canada) locale.

API Versions for Apex Classes, Apex Triggers, and Visualforce Pages

The International Components for Unicode (ICU) locale formats are available with API version 45.0 and later. To use the ICU locale formats in your customizations, update your Apex classes, Apex triggers, and Visualforce pages to the latest API version. If these components use API version 44.0 or earlier, they return Oracle's Java Development Kit (JDK) locale formats, which can cause data integrity issues and end-user confusion.

Custom Code and Locale Format Changes

Address, currency, date, datetime, integer, name, and time formats can change when a user changes locales. These formats can also change when the locale format standard changes or formats are updated. Learn how to avoid errors by using locale-neutral methods in your code and review examples. Then understand how to verify that your integrations work with new or changed formats.

ICU Locale Format Migration Tests

To avoid unexpected behavior after you migrate from Oracle's Java Development Kit (JDK) locale formats to International Components for Unicode (ICU) locale formats, test the ICU locales. When you migrate from JDK to ICU, the formats for some locales change. Use functional tests to verify existing functionality, and confirm that these formats appear correctly for each affected locale used in your org. Also, verify that integration with third parties works as expected, and test your installed packages with the new formats.

SEE ALSO:

[Locales Overview](#)

Adopt the ICU Locale Formats

To keep your org up to date, review the high-level process to successfully migrate to the new International Components for Unicode (ICU) locale formats. Some of the formats differ from the ones provided by Oracle's Java Development Kit (JDK). Understand how to determine the impact of changes on your org, and learn about the updates required to support the new formats.



Note: Orgs created in Winter '20 or later have ICU locale formats enabled by default. You can deactivate the update until it's auto-activated in Spring '24.

Here's the step-by-step process to migration from JDK to ICU locale formats.

1. Determine whether your org is using ICU or JDK locale formats.

Before you start, determine which formats you're using and whether these instructions apply to you.

EDITIONS

Available in: both Salesforce Classic (**not available in all orgs**) and Lightning Experience

Available in: all editions

2. Review the [considerations for adopting ICU](#).

Learn why Salesforce chose to adopt the ICU locale formats. Then review recommendations, including where to test and how to handle installed packages and custom code.

3. [Determine how the ICU locale formats affect your org](#).

Your migration effort depends on the locales used in your org. Use an SOQL query and report to identify the locales in use, then identify the specific changes for those locales to be included in testing.

4. [Enable the ICU locale formats](#) in a sandbox.

Before enabling the new formats in production, we highly recommend that you test the ICU locale formats in a sandbox.

5. [Update your Apex Classes, Apex Triggers, and Visualforce Pages to API version 45.0 or later](#) on page 95

To avoid data integrity issues and end-user confusion, update your Apex classes, Apex triggers, and Visualforce pages to API version 45.0 or later. If these components use API version 44.0 or earlier, they return Oracle's Java Development Kit (JDK) locale formats.

6. [Update custom code for the ICU locale formats](#).

When an org migrates from JDK locale formats to ICU locale formats, users see the new formats automatically in standard Salesforce fields and functionality. However, custom code can require adjustments. Learn how to use locale-neutral formats to prevent issues when locale formats change and see examples of common issues.

7. [Test the ICU locale formats](#) in a sandbox.

Run your standard functional tests and targeted tests of functionality that processes or produces locale formats. Test your results in each of the affected locales that is used in your org. If you find any issues, update your org and test again.

8. Notify your users and partners.

Let your users know when you plan to enable ICU in production and how the new locales can affect them. Otherwise, the differences between JDK and ICU locale formats can cause confusion. Reaching everyone can require multiple reminders before and after you enable ICU in production.

Also consider notifying your partners, especially if those partners send information to or extract information from Salesforce. Resolving issues related to integrations can require their assistance.

9. [Enable the ICU locale formats](#) in production.

After you test the ICU locale formats in a sandbox and identify the required adjustments, enable the ICU locale formats in production. Then make those same adjustments.

10. [Test the ICU locale formats](#) again in production.

To account for any variation between your sandbox and production orgs, run your standard functional tests. Also, test functionality that processes locale formats. If you find any issues, update your org, then test again. After you successfully validate the functionality in production, mark the release update as complete.

SEE ALSO:

[Locales Overview](#)

Determine Whether Your Org Uses ICU or JDK Locale Formats

To prepare for the move to the International Components for Unicode (ICU) library from Oracle's Java Development Kit (JDK) library, whether ICU is enabled in your org, or whether you're using JDK and must adopt the ICU locale formats. ICU is the new standard and enforced through a release update.

Orgs created in Winter '20 or later have ICU locale formats enabled by default. You can deactivate the update until it's enforced in Spring '24.

To determine whether your org is using ICU locale formats, check the status of the Enable ICU Locale Formats release update. Then verify a user interface setting.

1. From Setup, in the Quick Find Box, enter *Release Updates*, and then select **Release Updates**.
2. Click the **Needs Action** tab, and look for the Enable ICU Locale Formats release update.

If the Enable ICU Locale Formats release update is on that tab, click **Get Started** to see details about the update.

If you see "This update is now enabled for testing," then your org is using ICU locale formats. Otherwise, your org is using JDK locale formats.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

USER PERMISSIONS

To view release updates:

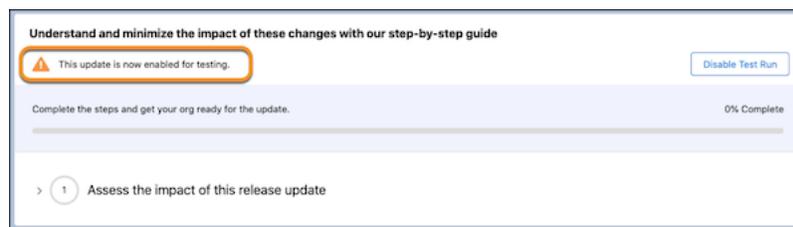
- View Setup and Configuration

To enable or disable release updates

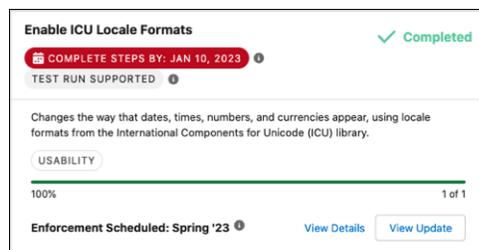
- Manage Release Updates

OR

Customize Application



If you don't find the release update on the Needs Action tab, click the **Archived** tab, and look for the Enable ICU Locale Formats release update. If the Enable ICU Locale Formats release update is marked complete, the release update was completed and your org is using ICU. The release update card has a green check mark and the word Completed in the upper right corner.



If your org is using JDK locale formats, we recommend that you test and adopt the ICU locale formats before they're enforced. If the Enable ICU formats for en_CA locale User Interface option is disabled, we recommend that you enable the option before the release update is enforced in Spring '24.

If your org is using ICU locale formats and the **Enable ICU formats for en_CA locale User Interface** option is enabled, your org is using the latest standard. No further action is required.

SEE ALSO:

[Adopt the ICU Locale Formats](#)

Considerations for Adopting the ICU Locale Formats

Learn why Salesforce chose to adopt the International Components for Unicode (ICU) locale formats. Understand why we recommend testing the new formats in a sandbox and enabling them in production before they're enforced. Then review recommendations on handling installed packages, custom code, and notifying your users.

Why Is Salesforce Making This Change?

Before Winter '20, new Salesforce orgs used the locale formats included with Oracle's Java Development Kit (JDK). This solution worked well, but it has a few issues. Most importantly, the JDK locale formats aren't consistent with internationalization best practices, and these JDK formats aren't updated regularly.

ICU is an international standard, maintained and governed by a global community. The new formats provide a consistent experience across the Salesforce platform and improve integration with ICU-compliant applications across the globe. By adopting the ICU locale formats, we keep Salesforce—and your business on Salesforce—up to date with these international standards.

Don't Wait for Enforcement

Salesforce enforces the ICU locale formats in all orgs in Spring '24 through the Enable ICU Locale Formats release update. Locales control the formats for dates, times, currencies, addresses, names, and numeric values. Moving from JDK to ICU locale formats can affect your users and cause misinterpretation of data. For this reason, we recommend that customers using JDK locale formats test and enable this change before it's enforced.

Test in a Sandbox

Before you enable the ICU locale formats in your production org, try them out in a sandbox org with API version 45.0 or higher. Testing in a sandbox can uncover any issues with custom code and third-party integrations.

Impact of Adopting a New API Version

To use the ICU locale formats, Apex classes, Apex triggers, and Visualforce pages that reference locale formats must use API version 45.0 or later. If your org contains items on API version 44.0 or earlier, update the API version to avoid data integrity issues and end-user confusion.

Updating the API version can include structural and behavior changes for objects and other code components. For example, the update can include new fields on an object, removal of a field, and changed behavior. We recommend upgrading the API version and completing thorough testing of all related functionality in a sandbox before you update production.

ICU and Inline Edits on Visualforce Pages

Inline edits on Visualforce pages always use the latest API version. Because of that behavior, when ICU is enabled, inline edits on Visualforce pages always use ICU locale formats, regardless of the page's API version. When a user makes an inline edit on a Visualforce page on API

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

version 44.0 or earlier and saves their changes, the user can receive a `ParseException` error. For example, "Invalid Date and Time." These errors don't cause data integrity issues, but the errors can frustrate users.

To avoid these errors when ICU is enabled, ensure that your custom Visualforce pages use API version 45.0 or later.

Installed Packages

Before you start testing, check with your package providers to make sure that all your installed packages are compatible with the ICU locale formats. If your package provider indicates that a fix for one of your installed packages is pending, factor that into your testing and activation timeline.

If you're a package provider, update the Apex classes, Apex triggers, and Visualforce pages in your packages to API version 45.0 or later. Update any custom code that requires or passes data in specific locale formats. Then test your packages in an org with ICU enabled. Verify that all changed formats appear as expected, and update your code as needed.

Custom Code

Many orgs contain custom code. Lightning Components allow you to customize Lightning Experience, the Salesforce mobile app, or to build your own standalone apps. With Apex, the options are even broader.

Apex is often used to:

- Create Web services.
- Create email services.
- Perform complex validation over multiple objects.
- Create complex business processes that aren't supported by workflow.
- Create custom transactional logic, which occurs over the entire transaction, not just with a single record or object.
- Attach custom logic to another operation. For example, attach custom logic to saving a record, so that it occurs whenever the operation is executed, regardless of where it originates in the user interface.

Also consider formula fields and areas where you can customize filters, such as object lookups. To search your Salesforce code, download the metadata. Then use a command-line interface such as [Salesforce CLI](#).

For more information on the steps to take to review and update your custom code, see [Custom Code and Locale Format Changes](#) in Salesforce Help. This section also provides examples of errors that can occur when custom code relies on specific date, time, and currency formats. Use this information to understand how to test custom functionality.

If an external developer or consultant created your custom code and you don't have a developer who can perform the assessment, start by testing the custom functionality. If you find issues, consider contracting with an external developer or consultant to assist with the evaluation of the custom code in your org.

Notify Your Users and Partners

Let your users know when you plan to enable ICU in production and how the new locales can affect them. Otherwise, the differences between JDK and ICU locale formats can cause confusion.

For example, with the Spanish (Honduras) locale, the short date format changes from MM-dd-yyyy to dd-MM-yyyy when you enable the ICU locale formats. Make sure that your users know about this change, or they can interpret 01-11-2021 as January 11, 2021 instead of November 1, 2021.

Reaching everyone can require multiple reminders before and after you enable ICU in production.

Also consider notifying your partners, especially if those partners send information to or extract information from Salesforce. Resolving issues related to integrations can require their assistance.

Use of Locale Formats

We provide a list of all possible locale formats, but not all formats are used in Salesforce. For example, almost all dates on standard Salesforce screens use the short date format, which can't be modified on standard screens.

Likewise, not all formats are available for use in custom code. In particular, the medium date format isn't available in Apex at this time.

SEE ALSO:

[Adopt the ICU Locale Formats](#)

[API Versions for Apex Classes, Apex Triggers, and Visualforce Pages](#)

[Custom Code and Locale Format Changes](#)

Determine the Locales in Use

To identify the locales used in your org, you can use an SOQL query, a report, or both. When locale formats change, your adoption effort depends on the locales used in your org. For example, when you migrate from Oracle's Java Development Kit (JDK) locale formats to International Components for Unicode (ICU) locale formats, or when existing locale formats change.

[Create a SOQL Query](#)

To gather details about locale use, like user count by locale, create a SOQL query

[Create a Custom Object for a Report](#)

To identify which users chose to use each locale, create a custom field on the User object. Then use that custom field to create a report that lists users by locale code.

[Identify Locales in Use by User](#)

To gather information about the users for each locale, use a custom field to create a report that lists users by locale code.

SEE ALSO:

[Identify Changes to Your Locales with ICU](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

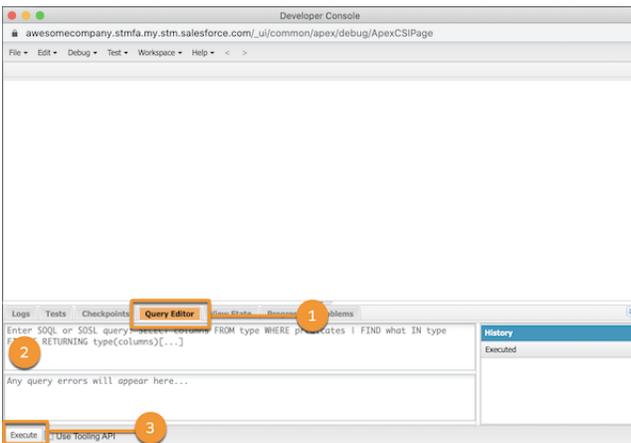
Available in: all editions

Create a SOQL Query

To gather details about locale use, like user count by locale, create a SOQL query

1. Click the gear icon (⚙️). Using Classic? Click your name in the upper right corner.
2. Click **Developer Console**.

The developer console opens in a new window.



3. To open the Query Editor panel, click **Query Editor** (1).

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

USER PERMISSIONS

To use the Developer Console:

- API Enabled AND View All Data

To use code search and run SOQL or SOSL on the query tab:

- API Enabled

To create, edit, and delete reports in private folders:

- Create and Customize Reports

To create, edit, and delete reports in public and private folders:

- Report Builder

OR

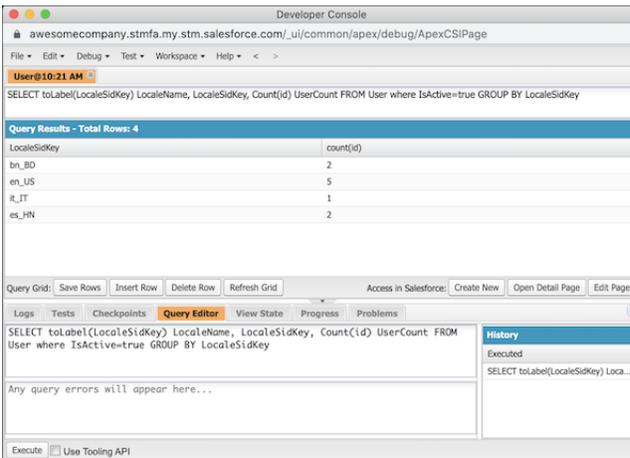
Report Builder (Lightning Experience)

- In the Query Editor panel (2), enter this query.

```
SELECT toLabel(LocaleSidKey) LocaleName, LocaleSidKey, Count(id) UserCount FROM User
where IsActive=true GROUP BY LocaleSidKey
```

- Click **Execute** (3).

Your results display in the Query Results grid in the Developer Console workspace.



In this example, there are 4 locales in use across 10 users: 2 users with bn_BD, 5 users with en_US, 1 user with it_IT, and 2 users with es_HN.

Create a Custom Object for a Report

To identify which users chose to use each locale, create a custom field on the User object. Then use that custom field to create a report that lists users by locale code.

- Click the gear icon (⚙️), and select **Setup**. Setup launches in a new tab.
- Click the **Object Manager** tab.
- From the list of objects, click **User**.
- Click **Fields & Relationships**, then click **New**.
- Select **Formula** as the data type, and click **Next**.
- For the Field Label, enter *Locale Code*.
- Ensure that **Add this field to existing custom report types that contain this entity** is selected.
- For Formula Return Type, select **Text**, and click **Next**.
- In the formula editor, enter `TEXT(LocaleSidKey)`, and click **Check Syntax**

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

USER PERMISSIONS

To view release updates:

- View Setup and Configuration

To enable or disable release updates

- Manage Release Updates

OR

Customize Application

The screenshot shows the 'New Custom Field' wizard in Salesforce, specifically Step 3: Enter formula. The main area contains a formula editor with the text 'Locale Code (Text)' entered. Below the editor, a green message states 'No syntax errors in merge fields or functions. (Compiled size: 4,289 characters)'. There are also input fields for 'Description' (with the text 'Locale code for the user's locale in personal settings'), 'Help Text', and a 'Blank Field Handling' section with two radio button options: 'Treat blank fields as zeros' and 'Treat blank fields as blanks' (which is selected). Navigation buttons for 'Previous', 'Next', and 'Cancel' are visible at the top and bottom of the wizard.

A green message confirms that no syntax errors were found.

10. Optionally, enter a description for the field such as *Locale code for the user's locale in personal settings*.
11. In Blank Field Handling, select **Treat blank fields as blanks**, and click **Next**.
12. Select the profiles that you want to grant edit access to this field. At minimum, select the **System Administrator** profile, and click **Next**.
13. Select the page layouts where you want to include this field, and click **Save**.

Identify Locales in Use by User

To gather information about the users for each locale, use a custom field to create a report that lists users by locale code.

To identify which users chose to use each locale, create a [custom field](#) on page 41 on the User object.

1. Click the App Launcher (☰).
2. In the search box, enter *Reports*, and select **Reports**.
3. Click **New Report**.
4. In the Report Type search box, enter *Users*, and click **Users**.
5. Click **Continue**.
The report opens in edit mode and shows a preview. The default report contains commonly used fields for the User object.
6. Group the users by locale code first. In the Outline pane, under Groups, enter *Locale Code* into the search box, and select **Locale Code**.
7. Then group the users by the locale name. In the Outline pane, under Groups, enter *Locale* into the search box, and select **Locale**.
8. To see what the report looks like, click **Refresh** above the report preview.

The preview shows the report grouped by locale code with the locale name beside it.

REPORT Users by Locale

Previewing a limited number of records. Run the report to see everything.

Locale Code	Locale	First Name	Last Name	Profile	Username	Alias
bn_BD (2)	Bangla (Bangladesh) (2)	Lochana	Singh	Chatter Free User	lsingh@awesomeco.com	lsingh
		Hardeep	Joshi	Chatter External User	hjoshi@awesomeco.com	hjoshi
Subtotal						
Subtotal						
en_US (3)	English (United States) (3)	Chloe	McKinney	System Administrator	cmkinney@awesomeco.com	cmkinney
		Sarah	Nibhanupudi	System Administrator	snibhanupudi@awesomeco.com	snibhan
		-	Chatter Expert	Chatter Free User	chatty.00ds7000000opdfmal.jzk5k7yaghs@chatter.salesforce.com	Chatter
Subtotal						
Subtotal						
es_HN (2)	Spanish (Honduras) (2)	Juanita	Hernandez	Standard User	jhernandez@awesomeco.com	jhern
		Elihu	Merino	Contract Manager	emerino@awesomeco.com	emerino
Subtotal						
Subtotal						
it_IT (1)	Italian (Italy) (1)	Galeazzo	Baresi	Marketing User	gbaresi@awesomeco.com	gbare
Subtotal						
Subtotal						
Total (8)						

Row Counts Detail Rows Subtotals Grand Total

9. Click **Save & Run**.

10. Enter a name for the report such as *Users by Locale Code*, select a folder to save the report, and then save your changes. Your report groups data by locale code and shows the full locale name for each code. This view can help you compare the locales in use in your org against the changes when you enable the ICU locale formats.

Report: Users
Users by Locale

List of our users, grouped by the locale they chose in personal settings.

Total Records: 8

Locale Code	Locale	First Name	Last Name	Profile	Username	Alias	Active	Last Login
bn_BD (2)	Bangla (Bangladesh) (2)	Lochana	Singh	Chatter Free User	lsingh@awesomeco.com	lsingh	<input checked="" type="checkbox"/>	-
		Hardeep	Joshi	Chatter External User	hjoshi@awesomeco.com	hjoshi	<input checked="" type="checkbox"/>	-
Subtotal								
Subtotal								
en_US (3)	English (United States) (3)	Chloe	McKinney	System Administrator	cmkinney@awesomeco.com	cmkinney	<input checked="" type="checkbox"/>	10/21/2021, 7:57 AM
		Sarah	Nibhanupudi	System Administrator	snibhanupudi@awesomeco.com	snibhan	<input checked="" type="checkbox"/>	12/3/2020, 7:49 AM
		-	Chatter Expert	Chatter Free User	chatty.00ds7000000opdfmal.jzk5k7yaghs@chatter.salesforce.com	Chatter	<input checked="" type="checkbox"/>	-
Subtotal								
Subtotal								
es_HN (2)	Spanish (Honduras) (2)	Juanita	Hernandez	Standard User	jhernandez@awesomeco.com	jhern	<input checked="" type="checkbox"/>	10/20/2021, 12:13 PM
		Elihu	Merino	Contract Manager	emerino@awesomeco.com	emerino	<input checked="" type="checkbox"/>	-
Subtotal								
Subtotal								
it_IT (1)	Italian (Italy) (1)	Galeazzo	Baresi	Marketing User	gbaresi@awesomeco.com	gbare	<input checked="" type="checkbox"/>	10/20/2021, 1:40 PM
Subtotal								
Subtotal								
Total (8)								

Row Counts Detail Rows Subtotals Grand Total

To view the users who chose one of the affected locales, filter the report by locale code.

Identify Changes to Your Locales with ICU

To ensure that you understand the impact of migrating from Oracle’s Java Development Kit (JDK) locale formats to International Components for Unicode (ICU) locale formats, determine the specific locale format changes.

The changes when you migrate from JDK to ICU depend on the locales used in your org. If you haven’t done so already, [determine the locales in use](#).

For a complete list of the differences between JDK and ICU locale formats, see [Differences Between JDK and ICU Locale Formats](#) in Salesforce Help.

The list of changes is long, and it’s unlikely that you use every one of those locales. Find the locales that your org uses by searching the Help page for the locale code. Then note the differences.

Here are some important tips.

- Not all locales change with ICU. In that case, the locale code isn’t listed on the Help page.
- We provide a list of all possible formats, but not all formats are used in Salesforce. For example, almost all dates on standard Salesforce screens use the short date format, and the medium date format is rarely used, if ever.
- Similarly, just because you see a format in the list doesn’t mean it’s available for your custom code. For example, the medium date format isn’t available in Apex.

Let’s look at an example analysis. Assume that the results of the SOQL query show users with the `bn_BD`, `en_US`, `es_NH`, and `it_IT` locales.

1. Go to [Differences Between JDK and ICU Locale Formats](#) in Salesforce Help.
2. In the browser window, search for `bn_BD`, the locale code for the Bangla (Bangladesh) locale.

The search shows no results, which means that there are no changes for that locale when migrating from JDK to ICU.

3. Search for the next locale code, `en_US`, for the English (United States) locale.

We find this section of the table.

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
English (United States) en_US	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 4:30 PM
	Date Time: Medium	Jan 28, 2008 4:30:05 PM	Jan 28, 2008, 4:30:05 PM
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 4:30:05 PM PST
	Currency: Negative	(\$1,234,567.57)	-\$1,234,567.57

Here we see that the datetime formats and the negative currency format changed. We can see that each datetime format has a comma after the year for the ICU format, but the JDK formats don’t have that comma. Also, the negative currency format changed from using parentheses to a negative sign.

4. Next, search for the next locale code, `es_NH`, for the Spanish (Honduras) locale.

We find this section of the table.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
Spanish (Honduras) es_HN	Date Time: Short	01-28-2008 04:30 PM	28/1/2008 16:30
	Date Time: Medium	01-28-2008 04:30:05 PM	28 ene. 2008 16:30:05
	Date Time: Long	01-28-2008 04:30:05 PM PST	28/1/2008 16:30:05 GMT-8
	Date: Short	01-28-2008	28/1/2008
	Date: Medium	01-28-2008	28 ene. 2008
	Time	04:30 PM	16:30
	Currency: Positive	L1,234,567.57	L 1,234,567.57
	Currency: Negative	(L1,234,567.57)	-L 1,234,567.57
	Accounting Currency: Positive	L1,234,567.57	L 1,234,567.57
	Accounting Currency: Negative	(L1,234,567.57)	-L 1,234,567.57

For this locale, date, datetime, time, and currency formats change with ICU. Notably, the month and the day switch positions in dates. Also, the time zone code changes in the long datetime format.

5. Search for `it_IT`, the locale code for the Italian (Italy) locale.

We find this section of the table.

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
Italian (Italy) it_IT	Date Time: Short	28/01/2008 16.30	28/01/2008, 16:30
	Date Time: Medium	28-gen-2008 16.30.05	28 gen 2008, 16:30:05
	Date Time: Long	28/01/2008 16.30.05 PST	28/01/2008, 16:30:05 GMT-8
	Date: Medium	28-gen-2008	28 gen 2008
	Time	16.30	16:30
	Currency: Positive	€ 1.234.567,57	1.234.567,57 €
	Currency: Negative	-€ 1.234.567,57	-1.234.567,57 €
	Accounting Currency: Positive	€ 1.234.567,57	1.234.567,57 €
	Accounting Currency: Negative	-€ 1.234.567,57	-1.234.567,57 €

Similar to the en_HN locale, date, time, and currency formats change with ICU for this locale. Sometimes the changes are subtle, so review the table carefully. In this case, the ICU locale format includes a comma after the year in datetime formats. However, a colon (:) also replaces the period (.) in the time and datetime formats.

In this example, we don't include the bn_BD, or Bangla (Bangladesh), locale in our testing. Based on the results, we plan to test with the en_US, es_HN, and it_IT locales. And now we know which formats to test for each locale.

SEE ALSO:

[Adopt the ICU Locale Formats](#)

Differences Between JDK and ICU Locale Formats

Here are all the differences between Oracle's Java Development Kit (JDK) locale formats and the International Components for Unicode (ICU) locale formats. The changes are listed by locale or platform-only language. By default, orgs created before Winter '20 use the locale formats provided by Oracle's JDK. ICU locale formats replace the JDK formats in Salesforce for all orgs in Spring '24, but you can adopt them now.



Note: We recommend viewing this information in Salesforce Help. Not all characters appear correctly in PDFs.

Changes to Supported Locale Formats

Supported Locales include a currency. Use them instead of language-only locales whenever possible.

- Not all locales have format changes when migrating from JDK to ICU. Locales without changes aren't included in the table.
- The table includes all the CLDR locale formats with changes between JDK and ICU. However, not all formats are used in Salesforce. For example, almost all dates on standard Salesforce screens use the short date format, and the medium date format is rarely used, if ever. Similarly, just because you see a format in the list doesn't mean it's available for your custom code. For example, the medium date format isn't available in Apex. We include list possible locale formats because external systems can use formats that aren't in use in Salesforce.
- Some locales have different formats for Currency and Accounting Currency. Accounting Currency is an ICU format used by accountants and often has a different representation for negative currency values than the standard Currency.

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
ar_JO	Date Time: Short	// :	// ,:
	Date Time: Medium	// ::	// ,::
	Date Time: Long	// - ::	// ,:: -
	Date: Short	//	//
	Date: Medium	//	//
	Date: Long	,	,
	Time	:	:
ar_LB	Date Time: Short	// :	// ,:
	Date Time: Medium	// ::	// ,::
	Date Time: Long	// - ::	// ,:: -

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Date: Short	//	//
	Date: Medium	//	//
	Date: Long	,	
	Time	:	:
)) ar_SA	Date Time: Short	// :	// , :
	Date Time: Medium	// ::	// , ::
	Date Time: Long	// - ::	// , :: -
	Date: Short	//	//
	Date: Medium	//	//
	Date: Long	,	
	Time	:	:
)) ar_SY	Date Time: Short	// :	// , :
	Date Time: Medium	// ::	// , ::
	Date Time: Long	// - ::	// , :: -
	Date: Short	//	//
	Date: Medium	//	//
	Date: Long	,	
	Time	:	:
Belarusian (Belarus) be_BY	Date Time: Short	28.1.2008 16.30	28.01.2008, 16:30
	Date Time: Medium	28.1.2008 16.30.05	28 Jan 2008 г., 16:30:05
	Date Time: Long	28.1.2008 16.30.05 PST	28.01.2008, 16:30:05 GMT-8
	Date: Short	28.1.2008	28.01.2008
	Date: Medium	28.1.2008	28 Jan 2008 г.
	Date: Long	Monday, 28, January 2008	28 January 2008 г.
	Time	16.30	16:30
	Currency: Positive	Py61 234 567,57	1 234 567,57 Br
	Currency: Negative	-Py61 234 567,57	-1 234 567,57 Br
	Accounting Currency: Positive	Py61 234 567,57	1 234 567,57 Br
	Accounting Currency: Negative	-Py61 234 567,57	-1 234 567,57 Br

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
Български (България) bg_BG	Date Time: Short	28.01.2008 16:30	28.01.2008 г., 16:30 ч.
	Date Time: Medium	28.01.2008 16:30:05	28.01.2008 г., 16:30:05 ч.
	Date Time: Long	28.01.2008 16:30:05 Гринуич-8	28.01.2008 г., 16:30:05 ч. Гринуич-8
	Date: Short	28.01.2008	28.01.2008 г.
	Date: Medium	28.01.2008	28.01.2008 г.
	Date: Long	28 януари 2008	28 януари 2008 г.
	Time	16:30	16:30 ч.
Català (Espanya) ca_ES	Date Time: Short	28/01/2008 16:30	28/1/2008 16:30
	Date Time: Medium	28/01/2008 16:30:05	28 de gen. 2008, 16:30:05
	Date Time: Long	28/01/2008 16:30:05 PST	28/1/2008 16:30:05 GMT-8
	Date: Short	28/01/2008	28/1/2008
	Date: Medium	28/01/2008	28 de gen. 2008
	Date: Long	28 / de gener / 2008	28 de gener de 2008
	Currency: Positive	€ 1.234.567,57	1.234.567,57 €
	Currency: Negative	-€ 1.234.567,57	-1.234.567,57 €
	Accounting Currency: Positive	€ 1.234.567,57	1.234.567,57 €
	Accounting Currency: Negative	-€ 1.234.567,57	(1.234.567,57 €)
Čeština (Česko) cs_CZ	Date Time: Short	28.1.2008 16:30	28.01.2008 16:30
	Date Time: Medium	28.1.2008 16:30:05	28. 1. 2008 16:30:05
	Date Time: Long	28.1.2008 16:30:05 PST	28.01.2008 16:30:05 PST
	Date: Short	28.1.2008	28.01.2008
	Date: Medium	28.1.2008	28. 1. 2008
	Number: Positive	1 234 567,57	1 234 567,567
	Number: Negative	-1 234 567,57	-1 234 567,567
	Currency: Positive	1 234 567,57 Kč	1 234 567,57 Kč
	Currency: Negative	-1 234 567,57 Kč	-1 234 567,57 Kč
	Accounting Currency: Positive	1 234 567,57 Kč	1 234 567,57 Kč
	Accounting Currency: Negative	-1 234 567,57 Kč	-1 234 567,57 Kč
Dansk (Danmark) da_DK	Date Time: Short	28-01-2008 16:30	28.01.2008 16.30
	Date Time: Medium	28-01-2008 16:30:05	28. jan. 2008 16.30.05

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Date Time: Long	28-01-2008 16:30:05 PST	28.01.2008 16.30.05 GMT-8
	Date: Short	28-01-2008	28.01.2008
	Date: Medium	28-01-2008	28. jan. 2008
	Time	16:30	16.30
	Currency: Positive	kr 1.234.567,57	1.234.567,57 kr.
	Currency: Negative	kr -1.234.567,57	-1.234.567,57 kr.
	Accounting Currency: Positive	kr 1.234.567,57	1.234.567,57 kr.
	Accounting Currency: Negative	kr -1.234.567,57	-1.234.567,57 kr.
Deutsch (Österreich) de_AT	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	28.01.2008 16:30:05	28.01.2008, 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 GMT-8
	Number: Positive	1.234.567,567	1 234 567,567
	Number: Negative	-1.234.567,567	-1 234 567,567
	Currency: Positive	€ 1.234.567,57	€ 1.234.567,57
	Currency: Negative	-€ 1.234.567,57	-€ 1.234.567,57
	Accounting Currency: Positive	€ 1.234.567,57	1.234.567,57 €
	Accounting Currency: Negative	-€ 1.234.567,57	-1.234.567,57 €
Deutsch (Schweiz) de_CH	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	28.01.2008 16:30:05	28.01.2008, 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 GMT-8
	Number: Positive	1'234'567.567	1'234'567.567
	Number: Negative	-1'234'567.567	-1'234'567.567
	Currency: Positive	SFr. 1'234'567.57	CHF 1'234'567.57
	Currency: Negative	SFr.-1'234'567.57	CHF-1'234'567.57
	Accounting Currency: Positive	SFr. 1'234'567.57	1'234'567.57 CHF
	Accounting Currency: Negative	SFr.-1'234'567.57	-1'234'567.57 CHF
Deutsch (Deutschland) de_DE	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	28.01.2008 16:30:05	28.01.2008, 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 GMT-8
	Currency: Positive	1.234.567,57 €	1.234.567,57 €

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Currency: Negative	-1.234.567,57 €	-1.234.567,57 €
	Accounting Currency: Positive	1.234.567,57 €	1.234.567,57 €
	Accounting Currency: Negative	-1.234.567,57 €	-1.234.567,57 €
Deutsch (Luxemburg) de_LU	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	28.01.2008 16:30:05	28.01.2008, 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 GMT-8
	Currency: Positive	1.234.567,57 €	1.234.567,57 €
	Currency: Negative	-1.234.567,57 €	-1.234.567,57 €
	Accounting Currency: Positive	1.234.567,57 €	1.234.567,57 €
	Accounting Currency: Negative	-1.234.567,57 €	-1.234.567,57 €
Ελληνικά (Κύπρος) el_CY	Date Time: Short	28/01/2008 4:30 MM	28/1/2008, 4:30 μ.μ.
	Date Time: Medium	28 Ιαν 2008 4:30:05 MM	28 Ιαν 2008, 4:30:05 μ.μ.
	Date Time: Long	28/01/2008 4:30:05 MM PST	28/1/2008, 4:30:05 μ.μ. GMT-8
	Date: Short	28/01/2008	28/1/2008
	Date: Long	28 Ιανουάριος, 2008	28 Ιανουαρίου 2008
	Time	4:30 MM	4:30 μ.μ.
	Currency: Positive	€1.234.567,57	1.234.567,57 €
	Currency: Negative	-€1.234.567,57	-1.234.567,57 €
	Accounting Currency: Positive	€1.234.567,57	1.234.567,57 €
	Accounting Currency: Negative	-€1.234.567,57	-1.234.567,57 €
Ελληνικά (Ελλάδα) el_GR	Date Time: Short	28/1/2008 4:30 μμ	28/1/2008, 4:30 μ.μ.
	Date Time: Medium	28 Ιαν 2008 4:30:05 μμ	28 Ιαν 2008, 4:30:05 μ.μ.
	Date Time: Long	28/1/2008 4:30:05 μμ PST	28/1/2008, 4:30:05 μ.μ. GMT-8
	Time	4:30 μμ	4:30 μ.μ.
	Currency: Positive	1.234.567,57 €	1.234.567,57 €
	Currency: Negative	-1.234.567,57 €	-1.234.567,57 €
	Accounting Currency: Positive	1.234.567,57 €	1.234.567,57 €
	Accounting Currency: Negative	-1.234.567,57 €	-1.234.567,57 €
English (Australia) en_AU	Date Time: Short	28/01/2008 4:30 PM	28/1/2008, 4:30 pm
	Date Time: Medium	28/01/2008 4:30:05 PM	28 Jan 2008, 4:30:05 pm

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Date Time: Long	28/01/2008 4:30:05 PM	28/1/2008, 4:30:05 pm GMT-8
	Date: Short	28/01/2008	28/1/2008
	Date: Medium	28/01/2008	28 Jan 2008
	Time	4:30 PM	4:30 pm
	Accounting Currency: Negative	-\$1,234,567.57	(\$1,234,567.57)
English (Barbados) en_BB	Date Time: Short	28/01/2008 16:30	28/01/2008, 4:30 pm
	Date Time: Medium	28/01/2008 16:30:05	28 Jan 2008, 4:30:05 pm
	Date Time: Long	28/01/2008 16:30:05 PST	28/01/2008, 4:30:05 pm GMT-8
	Date: Medium	28/01/2008	28 Jan 2008
English (Bermuda) en_BM	Date Time: Short	28/01/2008 16:30	28/01/2008, 4:30 pm
	Date Time: Medium	28/01/2008 16:30:05	28 Jan 2008, 4:30:05 pm
	Date Time: Long	28/01/2008 16:30:05 PST	28/01/2008, 4:30:05 pm GMT-8
	Date: Medium	28/01/2008	28 Jan 2008
English (Canada) en_CA	Date Time: Short	28/01/2008 4:30 PM	2008-01-28, 4:30 p.m.
	Date Time: Medium	28-Jan-2008 4:30:05 PM	Jan 28, 2008, 4:30:05 p.m.
	Date Time: Long	28/01/2008 4:30:05 PST PM	2008-01-28, 4:30:05 p.m. PST
	Date: Short	28/01/2008	2008-01-28
	Date: Medium	28-Jan-2008	Jan 28, 2008
	Time	4:30 PM	4:30 p.m.
	Accounting Currency: Negative	-\$1,234,567.57	(\$1,234,567.57)
English (United Kingdom) en_GB	Date Time: Short	28/01/2008 16:30	28/01/2008, 16:30
	Date Time: Medium	28-Jan-2008 16:30:05	28 Jan 2008, 16:30:05
	Date Time: Long	28/01/2008 16:30:05 PST	28/01/2008, 16:30:05 GMT-8
	Date: Medium	28-Jan-2008	28 Jan 2008
	Accounting Currency: Negative	-£1,234,567.57	(£1,234,567.57)
English (Ghana) en_GH	Date Time: Short	28/01/2008 16:30	28/01/2008, 4:30 pm
	Date Time: Medium	28/01/2008 16:30:05	28 Jan 2008, 4:30:05 pm
	Date Time: Long	28/01/2008 16:30:05 PST	28/01/2008, 4:30:05 pm GMT-8
	Date: Medium	28/01/2008	28 Jan 2008

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
English (Indonesia) en_ID	Date Time: Short	28/01/2008 16:30	28/01/2008, 16:30
	Date Time: Medium	28/01/2008 16:30:05	28 Jan 2008, 16:30:05
	Date Time: Long	28/01/2008 16:30:05 PST	28/01/2008, 16:30:05 GMT-8
	Date: Medium	28/01/2008	28 Jan 2008
	Date: Long	January 28, 2008	28 January 2008
	Time	4:30 PM	16:30
	Currency: Positive	IDR1,234,567.57	IDR 1,234,567.57
	Currency: Negative	-IDR1,234,567.57	-IDR 1,234,567.57
	Accounting Currency: Positive	IDR1,234,567.57	IDR 1,234,567.57
	Accounting Currency: Negative	-IDR1,234,567.57	(IDR 1,234,567.57)
English (Ireland) en_IE	Date Time: Short	28/01/2008 16:30	28/01/2008, 16:30
	Date Time: Medium	28-Jan-2008 16:30:05	28 Jan 2008, 16:30:05
	Date Time: Long	28/01/2008 16:30:05 PST	28/01/2008, 16:30:05 GMT-8
	Date: Medium	28-Jan-2008	28 Jan 2008
	Accounting Currency: Negative	-€1,234,567.57	(€1,234,567.57)
English (India) en_IN	Date Time: Short	28/1/2008 4:30 pm	28/01/2008, 4:30 pm
	Date Time: Medium	28 Jan, 2008 4:30:05 pm	28-Jan-2008, 4:30:05 pm
	Date Time: Long	28/1/2008 4:30:05 pm GMT-8	28/01/2008, 4:30:05 pm GMT-8
	Date: Short	28/1/2008	28/01/2008
	Date: Medium	28 Jan, 2008	28-Jan-2008
	Date: Long	28 January, 2008	28 January 2008
English (Italy) en_IT	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 16:30
	Date Time: Medium	Jan 28, 2008 4:30:05 PM	Jan 28, 2008, 16:30:05
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 16:30:05 PST
	Time	4:30 PM	16:30
	Accounting Currency: Negative	-€1,234,567.57	(€1,234,567.57)
English (Malta) en_MT	Date Time: Short	28/01/2008 16:30	28/01/2008, 16:30
	Date Time: Medium	28 Jan 2008 16:30:05	28 Jan 2008, 16:30:05
	Date Time: Long	28/01/2008 16:30:05 PST	28/01/2008, 16:30:05 GMT-8
	Accounting Currency: Negative	-€1,234,567.57	(€1,234,567.57)

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
English (Malaysia) en_MY	Date Time: Short	28/01/2008 16:30	28/01/2008, 4:30 pm
	Date Time: Medium	28/01/2008 16:30:05	28 Jan 2008, 4:30:05 pm
	Date Time: Long	28/01/2008 16:30:05 PST	28/01/2008, 4:30:05 pm GMT-8
	Date: Medium	28/01/2008	28 Jan 2008
English (Nigeria) en_NG	Date Time: Short	28/01/2008 16:30	28/01/2008, 16:30
	Date Time: Medium	28/01/2008 16:30:05	28 Jan 2008, 16:30:05
	Date Time: Long	28/01/2008 16:30:05 PST	28/01/2008, 16:30:05 GMT-8
	Date: Medium	28/01/2008	28 Jan 2008
English (New Zealand) en_NZ	Date Time: Short	28/01/2008 4:30 PM	28/01/2008, 4:30 pm
	Date Time: Medium	28/01/2008 4:30:05 PM	28/01/2008, 4:30:05 pm
	Date Time: Long	28/01/2008 4:30:05 PM	28/01/2008, 4:30:05 pm GMT-8
	Time	4:30 PM	4:30 pm
	Accounting Currency: Negative	-\$1,234,567.57	(\$1,234,567.57)
English (Philippines) en_PH	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 4:30 PM
	Date Time: Medium	01 28, 2008 4:30:05 PM	Jan 28, 2008, 4:30:05 PM
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 4:30:05 PM PST
	Date: Medium	01 28, 2008	Jan 28, 2008
	Currency: Positive	Php1,234,567.57	1,234,567.57
	Currency: Negative	(Php1,234,567.57)	- 1,234,567.57
	Accounting Currency: Positive	Php1,234,567.57	1,234,567.57
	Accounting Currency: Negative	(Php1,234,567.57)	(1,234,567.57)
English (Singapore) en_SG	Date Time: Short	28/01/2008 16:30	28/1/2008, 4:30 pm
	Date Time: Medium	28/01/2008 16:30:05	28 Jan 2008, 4:30:05 pm
	Date Time: Long	28/01/2008 16:30:05 PST	28/1/2008, 4:30:05 pm GMT-8
	Date: Short	28/01/2008	28/1/2008
	Date: Medium	28/01/2008	28 Jan 2008
	Date: Long	28 January, 2008	28 January 2008
	Time	4:30 PM	4:30 pm
	Accounting Currency: Negative	-\$1,234,567.57	(\$1,234,567.57)

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
English (United States) en_US	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 4:30 PM
	Date Time: Medium	Jan 28, 2008 4:30:05 PM	Jan 28, 2008, 4:30:05 PM
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 4:30:05 PM PST
	Currency: Negative	(\$1,234,567.57)	-\$1,234,567.57
English (South Africa) en_ZA	Date Time: Short	2008/01/28 4:30 PM	2008/01/28, 16:30
	Date Time: Medium	28 Jan 2008 4:30:05 PM	28 Jan 2008, 16:30:05
	Date Time: Long	2008/01/28 4:30:05 PM	2008/01/28, 16:30:05 GMT-8
	Time	4:30 PM	16:30
	Number: Positive	1,234,567.567	1 234 567,567
	Number: Negative	-1,234,567.567	-1 234 567,567
	Currency: Positive	R 1,234,567.57	R 1 234 567,57
	Currency: Negative	R-1,234,567.57	-R 1 234 567,57
	Accounting Currency: Positive	R 1,234,567.57	R 1 234 567,57
	Accounting Currency: Negative	R-1,234,567.57	(R 1 234 567,57)
Español (Argentina) es_AR	Date Time: Short	28/01/2008 16:30	28/1/2008, 16:30
	Date Time: Medium	28/01/2008 16:30:05	28 ene 2008 16:30:05
	Date Time: Long	28/01/2008 16:30:05 PST	28/1/2008, 16:30:05 GMT-8
	Date: Short	28/01/2008	28/1/2008
	Date: Medium	28/01/2008	28 ene 2008
	Currency: Positive	\$1.234.567,57	\$ 1.234.567,57
	Currency: Negative	-\$1.234.567,57	-\$ 1.234.567,57
	Accounting Currency: Positive	\$1.234.567,57	\$ 1.234.567,57
	Accounting Currency: Negative	-\$1.234.567,57	(\$ 1.234.567,57)
Español (Bolivia) es_BO	Date Time: Short	28-01-2008 04:30 PM	28/1/2008, 16:30
	Date Time: Medium	28-01-2008 04:30:05 PM	28 ene de 2008 16:30:05
	Date Time: Long	28-01-2008 04:30:05 PM PST	28/1/2008, 16:30:05 GMT-8
	Date: Short	28-01-2008	28/1/2008
	Date: Medium	28-01-2008	28 ene de 2008
	Time	04:30 PM	16:30
	Currency: Positive	B\$1.234.567,57	Bs 1.234.567,57

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Currency: Negative	(B\$1.234.567,57)	-Bs 1.234.567,57
	Accounting Currency: Positive	B\$1.234.567,57	Bs 1.234.567,57
	Accounting Currency: Negative	(B\$1.234.567,57)	-Bs 1.234.567,57
Español (Chile) es_CL	Date Time: Short	28-01-2008 16:30	28-01-2008, 16:30
	Date Time: Long	28-01-2008 16:30:05 PST	28-01-2008, 16:30:05 GMT-8
	Currency: Positive	Ch\$1.234.567,57	\$1.234.567,57
	Currency: Negative	Ch\$-1.234.567,57	-\$1.234.567,57
	Accounting Currency: Positive	Ch\$1.234.567,57	\$1.234.567,57
	Accounting Currency: Negative	Ch\$-1.234.567,57	-\$1.234.567,57
Español (Colombia) es_CO	Date Time: Short	28/01/2008 04:30 PM	28/01/2008, 4:30 p. m.
	Date Time: Medium	28/01/2008 04:30:05 PM	28/01/2008, 4:30:05 p. m.
	Date Time: Long	28/01/2008 04:30:05 PM PST	28/01/2008, 4:30:05 p. m. GMT-8
	Time	04:30 PM	4:30 p. m.
	Currency: Positive	\$1.234.567,57	\$ 1.234.567,57
	Currency: Negative	(\$1.234.567,57)	-\$ 1.234.567,57
	Accounting Currency: Negative	(\$1.234.567,57)	-\$1.234.567,57
Español (Costa Rica) es_CR	Date Time: Short	28/01/2008 04:30 PM	28/1/2008, 16:30
	Date Time: Medium	28/01/2008 04:30:05 PM	28 ene 2008 16:30:05
	Date Time: Long	28/01/2008 04:30:05 PM PST	28/1/2008, 16:30:05 GMT-8
	Date: Short	28/01/2008	28/1/2008
	Date: Medium	28/01/2008	28 ene 2008
	Time	04:30 PM	16:30
	Number: Positive	1,234,567.567	1 234 567,567
	Number: Negative	-1,234,567.567	-1 234 567,567
	Currency: Positive	C1,234,567.57	1 234 567,57
	Currency: Negative	(C1,234,567.57)	- 1 234 567,57
	Accounting Currency: Positive	C1,234,567.57	1 234 567,57
	Accounting Currency: Negative	(C1,234,567.57)	- 1 234 567,57
Español (República Dominicana)	Date Time: Short	28/01/2008 04:30 PM	28/1/2008, 4:30 p. m.

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
es_DO	Date Time: Medium	28/01/2008 04:30:05 PM	28 ene 2008 4:30:05 p. m.
	Date Time: Long	28/01/2008 04:30:05 PM PST	28/1/2008, 4:30:05 p. m. GMT-8
	Date: Short	28/01/2008	28/1/2008
	Date: Medium	28/01/2008	28 ene 2008
	Time	04:30 PM	4:30 p. m.
	Currency: Negative	(RD\$1,234,567.57)	-RD\$1,234,567.57
Español (Ecuador)	Date Time: Short	28/01/2008 16:30	28/1/2008, 16:30
es_EC	Date Time: Medium	28/01/2008 16:30:05	28 ene 2008 16:30:05
	Date Time: Long	28/01/2008 16:30:05 PST	28/1/2008, 16:30:05 GMT-8
	Date: Short	28/01/2008	28/1/2008
	Date: Medium	28/01/2008	28 ene 2008
	Accounting Currency: Negative	\$-1.234.567,57	-\$1.234.567,57
Español (España)	Date Time: Short	28/01/2008 16:30	28/1/2008, 16:30
es_ES	Date Time: Medium	28-ene-2008 16:30:05	28 ene 2008, 16:30:05
	Date Time: Long	28/01/2008 16:30:05 PST	28/1/2008, 16:30:05 GMT-8
	Date: Short	28/01/2008	28/1/2008
	Date: Medium	28-ene-2008	28 ene 2008
	Currency: Positive	1.234.567,57 €	1.234.567,57 €
	Currency: Negative	-1.234.567,57 €	-1.234.567,57 €
	Accounting Currency: Positive	1.234.567,57 €	1.234.567,57 €
	Accounting Currency: Negative	-1.234.567,57 €	-1.234.567,57 €
Español (Guatemala)	Date Time: Short	28/01/2008 04:30 PM	28/01/2008, 16:30
	Date Time: Medium	28/01/2008 04:30:05 PM	28/01/2008 16:30:05
	Date Time: Long	28/01/2008 04:30:05 PM PST	28/01/2008, 16:30:05 GMT-8
	Time	04:30 PM	16:30
	Currency: Positive	Q1,234,567.57	Q 1,234,567.57
	Currency: Negative	(Q1,234,567.57)	-Q 1,234,567.57
	Accounting Currency: Positive	Q1,234,567.57	Q 1,234,567.57
	Accounting Currency: Negative	(Q1,234,567.57)	-Q 1,234,567.57

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
Español (Honduras) es_HN	Date Time: Short	01-28-2008 04:30 PM	28/1/2008, 16:30
	Date Time: Medium	01-28-2008 04:30:05 PM	28 ene 2008 16:30:05
	Date Time: Long	01-28-2008 04:30:05 PM PST	28/1/2008, 16:30:05 GMT-8
	Date: Short	01-28-2008	28/1/2008
	Date: Medium	01-28-2008	28 ene 2008
	Time	04:30 PM	16:30
	Currency: Positive	L1,234,567.57	L 1,234,567.57
	Currency: Negative	(L1,234,567.57)	-L 1,234,567.57
	Accounting Currency: Positive	L1,234,567.57	L 1,234,567.57
	Accounting Currency: Negative	(L1,234,567.57)	-L 1,234,567.57
Español (México) es_MX	Date Time: Short	28/01/2008 04:30 PM	28/01/2008, 16:30
	Date Time: Medium	28/01/2008 04:30:05 PM	28 ene 2008 16:30:05
	Date Time: Long	28/01/2008 04:30:05 PM PST	28/01/2008, 16:30:05 GMT-8
	Date: Medium	28/01/2008	28 ene 2008
	Time	04:30 PM	16:30
Español (Nicaragua) es_NI	Date Time: Short	01-28-2008 04:30 PM	28/1/2008, 16:30
	Date Time: Medium	01-28-2008 04:30:05 PM	28 ene 2008 16:30:05
	Date Time: Long	01-28-2008 04:30:05 PM PST	28/1/2008, 16:30:05 GMT-8
	Date: Short	01-28-2008	28/1/2008
	Date: Medium	01-28-2008	28 ene 2008
	Time	04:30 PM	16:30
	Currency: Positive	₡C1,234,567.57	C\$1,234,567.57
	Currency: Negative	(₡C1,234,567.57)	-C\$1,234,567.57
	Accounting Currency: Positive	₡C1,234,567.57	C\$1,234,567.57
	Accounting Currency: Negative	(₡C1,234,567.57)	-C\$1,234,567.57
Español (Panamá) es_PA	Date Time: Short	01/28/2008 04:30 PM	01/28/2008, 4:30 p. m.
	Date Time: Medium	01/28/2008 04:30:05 PM	01/28/2008 4:30:05 p. m.
	Date Time: Long	01/28/2008 04:30:05 PM PST	01/28/2008, 4:30:05 p. m. GMT-8
	Time	04:30 PM	4:30 p. m.
	Currency: Positive	B1,234,567.57	B/. 1,234,567.57

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Currency: Negative	(B1,234,567.57)	-B/. 1,234,567.57
	Accounting Currency: Positive	B1,234,567.57	B/. 1,234,567.57
	Accounting Currency: Negative	(B1,234,567.57)	-B/. 1,234,567.57
Español (Perú) es_PE	Date Time: Short	28/01/2008 04:30 p. m.	28/01/2008, 16:30
	Date Time: Medium	28/01/2008 04:30:05 p. m.	28 ene. 2008 16:30:05
	Date Time: Long	28/01/2008 04:30:05 p. m. GMT-8	28/01/2008, 16:30:05 GMT-8
	Date: Medium	28/01/2008	28 ene. 2008
	Time	04:30 p. m.	16:30
Español (Puerto Rico) es_PR	Date Time: Short	01-28-2008 04:30 PM	01/28/2008, 4:30 p. m.
	Date Time: Medium	01-28-2008 04:30:05 PM	01/28/2008 4:30:05 p. m.
	Date Time: Long	01-28-2008 04:30:05 PM PST	01/28/2008, 4:30:05 p. m. GMT-8
	Date: Short	01-28-2008	01/28/2008
	Date: Medium	01-28-2008	01/28/2008
	Time	04:30 PM	4:30 p. m.
	Currency: Negative	(\$1,234,567.57)	-\$1,234,567.57
	Accounting Currency: Negative	(\$1,234,567.57)	-\$1,234,567.57
Español (Paraguay) es_PY	Date Time: Short	28/01/2008 04:30 PM	28/1/2008, 16:30
	Date Time: Medium	28/01/2008 04:30:05 PM	28 ene. 2008 16:30:05
	Date Time: Long	28/01/2008 04:30:05 PM PST	28/1/2008, 16:30:05 GMT-8
	Date: Short	28/01/2008	28/1/2008
	Date: Medium	28/01/2008	28 ene. 2008
	Time	04:30 PM	16:30
	Currency: Positive	G1.234.567,57	Gs. 1.234.567,57
	Currency: Negative	(G1.234.567,57)	Gs. -1.234.567,57
	Accounting Currency: Positive	G1.234.567,57	Gs. 1.234.567,57
	Accounting Currency: Negative	(G1.234.567,57)	-Gs. 1.234.567,57
Español (El Salvador) es_SV	Default Currency	Colón salvadoreño: SVC	Dólar estadounidense: USD
	Date Time: Short	01-28-2008 04:30 PM	28/1/2008, 16:30
	Date Time: Medium	01-28-2008 04:30:05 PM	28 ene 2008 16:30:05
	Date Time: Long	01-28-2008 04:30:05 PM PST	28/1/2008, 16:30:05 GMT-8

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Date: Short	01-28-2008	28/1/2008
	Date: Medium	01-28-2008	28 ene 2008
	Time	04:30 PM	16:30
	Currency: Positive	C1,234,567.57	\$1,234,567.57
	Currency: Negative	(C1,234,567.57)	-\$1,234,567.57
	Accounting Currency: Positive	C1,234,567.57	\$1,234,567.57
	Accounting Currency: Negative	(C1,234,567.57)	-\$1,234,567.57
Español (Estados Unidos) es_US	Date Time: Short	1/28/2008 4:30 p.m.	28/1/2008, 4:30 p. m.
	Date Time: Medium	ene 28, 2008 4:30:05 p.m.	28 ene 2008, 4:30:05 p. m.
	Date Time: Long	1/28/2008 4:30:05 p.m. PST	28/1/2008, 4:30:05 p. m. PST
	Date: Short	1/28/2008	28/1/2008
	Date: Medium	ene 28, 2008	28 ene 2008
	Time	4:30 p.m.	4:30 p. m.
	Currency: Positive	US\$1,234,567.57	\$1,234,567.57
	Currency: Negative	(US\$1,234,567.57)	-\$1,234,567.57
	Accounting Currency: Positive	US\$1,234,567.57	\$1,234,567.57
	Accounting Currency: Negative	(US\$1,234,567.57)	-\$1,234,567.57
Español (Uruguay) es_UY	Date Time: Short	28/01/2008 04:30 PM	28/1/2008, 16:30
	Date Time: Medium	28/01/2008 04:30:05 PM	28 ene. 2008 16:30:05
	Date Time: Long	28/01/2008 04:30:05 PM PST	28/1/2008, 16:30:05 GMT-8
	Date: Short	28/01/2008	28/1/2008
	Date: Medium	28/01/2008	28 ene. 2008
	Time	04:30 PM	16:30
	Currency: Positive	NU\$ 1.234.567,57	\$ 1.234.567,57
	Currency: Negative	(NU\$1.234.567,57)	-\$ 1.234.567,57
	Accounting Currency: Positive	NU\$ 1.234.567,57	\$ 1.234.567,57
	Accounting Currency: Negative	(NU\$1.234.567,57)	(\$ 1.234.567,57)
Español (Venezuela) es_VE	Date Time: Short	28/01/2008 04:30 PM	28/1/2008, 4:30 p. m.
	Date Time: Medium	28/01/2008 04:30:05 PM	28 ene. 2008 4:30:05 p. m.
	Date Time: Long	28/01/2008 04:30:05 PM PST	28/1/2008, 4:30:05 p. m. GMT-8

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Date: Short	28/01/2008	28/1/2008
	Date: Medium	28/01/2008	28 ene. 2008
	Time	04:30 PM	4:30 p. m.
	Currency: Positive	Bs.S.1.234.567,57	Bs.S 1.234.567,57
	Currency: Negative	Bs.S. -1.234.567,57	Bs.S-1.234.567,57
	Accounting Currency: Positive	Bs.S.1.234.567,57	Bs.S 1.234.567,57
	Accounting Currency: Negative	Bs.S. -1.234.567,57	-Bs.S 1.234.567,57
Eesti (Eesti) et_EE	Date Time: Medium	28.01.2008 16:30:05	28. jaan 2008 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008 16:30:05 GMT –8
	Date: Medium	28.01.2008	28. jaan 2008
	Date: Long	esmaspäev, 28. jaanuar 2008. a	28. jaanuar 2008
	Number: Negative	-1 234 567,567	–1 234 567,567
	Currency: Positive	1 234 567,57 €	1 234 567,57 €
	Currency: Negative	-1 234 567,57 €	–1 234 567,57 €
	Accounting Currency: Positive	1 234 567,57 €	1 234 567,57 €
	Accounting Currency: Negative	-1 234 567,57 €	(1 234 567,57 €)
Suomi (Suomi) fi_FI	Date Time: Short	28.1.2008 16:30	28.1.2008 16.30
	Date Time: Medium	28.1.2008 16:30:05	28.1.2008 klo 16.30.05
	Date Time: Long	28.1.2008 klo 16.30.05	28.1.2008 16.30.05 UTC-8
	Time	16:30	16.30
	Number: Negative	-1 234 567,567	–1 234 567,567
	Currency: Positive	1 234 567,57 €	1 234 567,57 €
	Currency: Negative	-1 234 567,57 €	–1 234 567,57 €
	Accounting Currency: Positive	1 234 567,57 €	1 234 567,57 €
	Accounting Currency: Negative	-1 234 567,57 €	–1 234 567,57 €
Français (Belgique) fr_BE	Date Time: Medium	28-janv.-2008 16:30:05	28 janv. 2008, 16:30:05
	Date Time: Long	28/01/2008 16:30:05 PST	28/01/2008 16:30:05 UTC–8
	Date: Medium	28-janv.-2008	28 janv. 2008
	Number: Positive	1.234.567,567	1 234 567,567
	Number: Negative	-1.234.567,567	-1 234 567,567

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Currency: Positive	1.234.567,57 €	1 234 567,57 €
	Currency: Negative	-1.234.567,57 €	-1 234 567,57 €
	Accounting Currency: Positive	1.234.567,57 €	1 234 567,57 €
	Accounting Currency: Negative	-1.234.567,57 €	(1 234 567,57 €)
Français (Canada) fr_CA	Date Time: Short	2008-01-28 16:30	2008-01-28 16 h 30
	Date Time: Medium	2008-01-28 16:30:05	28 janv. 2008, 16 h 30 min 05 s
	Date Time: Long	2008-01-28 16:30:05 HNP	2008-01-28 16 h 30 min 05 s HNP
	Date: Medium	2008-01-28	28 janv. 2008
	Time	16:30	16 h 30
	Currency: Positive	1 234 567,57 \$	1 234 567,57 \$
	Currency: Negative	(1 234 567,57\$)	-1 234 567,57 \$
	Accounting Currency: Positive	1 234 567,57 \$	1 234 567,57 \$
	Accounting Currency: Negative	(1 234 567,57\$)	(1 234 567,57 \$)
Français (Suisse) fr_CH	Date Time: Medium	28 janv. 2008 16:30:05	28 janv. 2008, 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008 16:30:05 UTC-8
	Date: Long	28. janvier 2008	28 janvier 2008
	Number: Positive	1'234'567.567	1 234 567,567
	Number: Negative	-1'234'567.567	-1 234 567,567
	Currency: Positive	SFr. 1'234'567.57	1 234 567.57 CHF
	Currency: Negative	SFr.-1'234'567.57	-1 234 567.57 CHF
	Accounting Currency: Positive	SFr. 1'234'567.57	1 234 567.57 CHF
Accounting Currency: Negative	SFr.-1'234'567.57	(1 234 567.57 CHF)	
Français (France) fr_FR	Date Time: Medium	28 janv. 2008 16:30:05	28 janv. 2008, 16:30:05
	Date Time: Long	28/01/2008 16:30:05 PST	28/01/2008 16:30:05 UTC-8
	Number: Positive	1 234 567,567	1 234 567,567
	Number: Negative	-1 234 567,567	-1 234 567,567
	Currency: Positive	1 234 567,57 €	1 234 567,57 €
	Currency: Negative	-1 234 567,57 €	-1 234 567,57 €
	Accounting Currency: Positive	1 234 567,57 €	1 234 567,57 €
Accounting Currency: Negative	-1 234 567,57 €	(1 234 567,57 €)	

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
Gaeilge (Éire) ga_IE	Accounting Currency: Negative	-€1,234,567.57	(€1,234,567.57)
() hi_IN	Date Time: Short	28/1/2008 4:30 pm	28/1/2008, 4:30 pm
	Date Time: Medium	28 , 2008 4:30:05 pm	28 2008, 4:30:05 pm
	Date Time: Long	28/1/2008 4:30:05 pm GMT-8	28/1/2008, 4:30:05 pm GMT-8
	Date: Medium	28 , 2008	28 2008
	Date: Long	28 , 2008	28 2008
Hmong (United States) hmn_US	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 4:30 PM
	Date Time: Medium	Jan 28, 2008 4:30:05 PM	Jan 28, 2008, 4:30:05 PM
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 4:30:05 PM PST
	Currency: Positive	USD 1,234,567.57	\$1,234,567.57
	Currency: Negative	-USD 1,234,567.57	-\$1,234,567.57
	Accounting Currency: Positive	USD 1,234,567.57	\$1,234,567.57
	Accounting Currency: Negative	-USD 1,234,567.57	(\$1,234,567.57)
Hrvatski (Hrvatska) hr_HR	Date Time: Short	28.01.2008. 16:30	28. 01. 2008. 16:30
	Date Time: Medium	28.01.2008. 16:30:05	28. sij 2008. 16:30:05
	Date Time: Long	28.01.2008. 16:30:05 PST	28. 01. 2008. 16:30:05 GMT -8
	Date: Short	28.01.2008.	28. 01. 2008.
	Date: Medium	28.01.2008.	28. sij 2008.
	Date: Long	2008. siječnja 28	28. siječnja 2008.
	Number: Negative	-1.234.567,567	-1.234.567,567
	Currency: Positive	€ 1.234.567,57	1.234.567,57 EUR
	Currency: Negative	-€ 1.234.567,57	-1.234.567,57 EUR
	Accounting Currency: Positive	€ 1.234.567,57	1.234.567,57 EUR
	Accounting Currency: Negative	-€ 1.234.567,57	-1.234.567,57 EUR
Hrvatski (Hrvatska, HRK) hr_HR_HRK	Date Time: Short	28.01.2008. 16:30	28. 01. 2008. 16:30
	Date Time: Medium	28.01.2008. 16:30:05	28. sij 2008. 16:30:05
	Date Time: Long	28.01.2008. 16:30:05 PST	28. 01. 2008. 16:30:05 GMT -8
	Date: Short	28.01.2008.	28. 01. 2008.
	Date: Medium	28.01.2008.	28. sij 2008.

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Date: Long	2008. siječnja 28	28. siječnja 2008.
	Number: Negative	-1.234.567,567	–1.234.567,567
	Currency: Positive	Kn 1.234.567,57	1.234.567,57 kn
	Currency: Negative	-Kn 1.234.567,57	–1.234.567,57 kn
	Accounting Currency: Positive	Kn 1.234.567,57	1.234.567,57 kn
	Accounting Currency: Negative	-Kn 1.234.567,57	–1.234.567,57 kn
Haitian Creole (Haiti) ht_HT	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 16:30
	Date Time: Medium	Jan 28, 2008 4:30:05 PM	Jan 28, 2008, 16:30:05
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 16:30:05 PST
	Time	4:30 PM	16:30
	Currency: Positive	HTG 1,234,567.57	HTG 1,234,567.57
	Currency: Negative	-HTG 1,234,567.57	-HTG 1,234,567.57
	Accounting Currency: Positive	HTG 1,234,567.57	HTG 1,234,567.57
	Accounting Currency: Negative	-HTG 1,234,567.57	(HTG 1,234,567.57)
Haitian Creole (United States) ht_US	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 4:30 PM
	Date Time: Medium	Jan 28, 2008 4:30:05 PM	Jan 28, 2008, 4:30:05 PM
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 4:30:05 PM PST
	Currency: Positive	USD 1,234,567.57	\$1,234,567.57
	Currency: Negative	-USD 1,234,567.57	-\$1,234,567.57
	Accounting Currency: Positive	USD 1,234,567.57	\$1,234,567.57
	Accounting Currency: Negative	-USD 1,234,567.57	(\$1,234,567.57)
Magyar (Magyarország) hu_HU	Date Time: Short	2008.01.28. 16:30	2008. 01. 28. 16:30
	Date Time: Medium	2008.01.28. 16:30:05	2008. jan. 28. 16:30:05
	Date Time: Long	2008.01.28. 16:30:05 PST	2008. 01. 28. 16:30:05 GMT-8
	Date: Short	2008.01.28.	2008. 01. 28.
	Date: Medium	2008.01.28.	2008. jan. 28.
	Currency: Positive	1 234 567,57 Ft	1 234 567,57 Ft
	Currency: Negative	-1 234 567,57 Ft	-1 234 567,57 Ft
	Accounting Currency: Positive	1 234 567,57 Ft	1 234 567,57 Ft
	Accounting Currency: Negative	-1 234 567,57 Ft	-1 234 567,57 Ft

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
Indonesia (Indonesia) in_ID	Date Time: Short	28/01/2008 16:30	28/01/2008 16.30
	Date Time: Medium	28 Jan 2008 16:30:05	28 Jan 2008 16.30.05
	Date Time: Long	28/01/2008 16:30:05	28/01/2008 16.30.05 PST
	Time	16:30	16.30
	Currency: Positive	Rp1.234.567,57	Rp 1.234.567,57
	Currency: Negative	-Rp1.234.567,57	-Rp 1.234.567,57
	Accounting Currency: Positive	Rp1.234.567,57	Rp 1.234.567,57
	Accounting Currency: Negative	-Rp1.234.567,57	-Rp 1.234.567,57
Íslenska (Ísland) is_IS	Date Time: Short	28.1.2008 16:30	28.1.2008, 16:30
	Date Time: Medium	28.1.2008 16:30:05	28. jan. 2008, 16:30:05
	Date Time: Long	28.1.2008 16:30:05 PST	28.1.2008, 16:30:05 GMT-8
	Date: Medium	28.1.2008	28. jan. 2008
	Currency: Positive	1.234.567,57 kr.	1.234.567,57 ISK
	Currency: Negative	-1.234.567,57 kr.	-1.234.567,57 ISK
	Accounting Currency: Positive	1.234.567,57 kr.	1.234.567,57 ISK
	Accounting Currency: Negative	-1.234.567,57 kr.	-1.234.567,57 ISK
Italiano (Svizzera) it_CH	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	28-gen-2008 16:30:05	28 gen 2008, 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 GMT-8
	Date: Medium	28-gen-2008	28 gen 2008
	Date: Long	28. gennaio 2008	28 gennaio 2008
	Number: Positive	1'234'567.567	1'234'567.567
	Number: Negative	-1'234'567.567	-1'234'567.567
	Currency: Positive	SFr. 1'234'567.57	CHF 1'234'567.57
	Currency: Negative	SFr.-1'234'567.57	CHF-1'234'567.57
	Accounting Currency: Positive	SFr. 1'234'567.57	1'234'567.57 CHF
Accounting Currency: Negative	SFr.-1'234'567.57	-1'234'567.57 CHF	
Italiano (Italia) it_IT	Date Time: Short	28/01/2008 16.30	28/01/2008, 16:30
	Date Time: Medium	28-gen-2008 16.30.05	28 gen 2008, 16:30:05
	Date Time: Long	28/01/2008 16.30.05 PST	28/01/2008, 16:30:05 GMT-8

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT	
	Date: Medium	28-gen-2008	28 gen 2008	
	Time	16.30	16:30	
	Currency: Positive	€ 1.234.567,57	1.234.567,57 €	
	Currency: Negative	-€ 1.234.567,57	-1.234.567,57 €	
	Accounting Currency: Positive	€ 1.234.567,57	1.234.567,57 €	
	Accounting Currency: Negative	-€ 1.234.567,57	-1.234.567,57 €	
)) iw_IL	Date Time: Short	16:30 28/01/2008	28.1.2008, 16:30	
	Date Time: Medium	16:30:05 28/01/2008	28 2008, 16:30:05	
	Date Time: Long	16:30:05 PST 28/01/2008	28.1.2008, 16:30:05 GMT-8	
	Date: Short	28/01/2008	28.1.2008	
	Date: Medium	28/01/2008	28 2008	
	Date: Long	28 2008	28 2008	
	Number: Negative	-1,234,567.567	-1,234,567.567	
	Currency: Positive	1,234,567.57 "	1,234,567.57	
	Currency: Negative	-1,234,567.57 "	-1,234,567.57	
	Accounting Currency: Positive	1,234,567.57 "	1,234,567.57	
	Accounting Currency: Negative	-1,234,567.57 "	-1,234,567.57	
	() ja_JP	Date Time: Long	2008/01/28 16:30:05 PST	2008/01/28 16:30:05 GMT-8
		Date: Long	2008/01/28	2008年1月28日
Accounting Currency: Negative		-¥1,234,567.57	(¥1,234,567.57)	
() ko_KR	Date Time: Short	2008. 1. 28 오후 4:30	2008. 1. 28. 오후 4:30	
	Date Time: Medium	2008. 1. 28 오후 4:30:05	2008. 1. 28. 오후 4:30:05	
	Date Time: Long	2008. 1. 28 오후 4시 30분 05초	2008. 1. 28. 오후 4시 30분 5초 GMT-8	
	Date: Short	2008. 1. 28	2008. 1. 28.	
	Date: Medium	2008. 1. 28	2008. 1. 28.	
	Date: Long	2008년 1월 28일 (월)	2008년 1월 28일	
	Currency: Positive	₩1,234,567.57	₩1,234,567.57	
	Currency: Negative	-₩1,234,567.57	-₩1,234,567.57	
	Accounting Currency: Positive	₩1,234,567.57	₩1,234,567.57	

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Accounting Currency: Negative	–₩1,234,567.57	(₩1,234,567.57)
Lietuvių (Lietuva) lt_LT	Date Time: Short	2008.1.28 16:30	2008-01-28 16:30
	Date Time: Medium	2008-01-28 16.30.05	2008-01-28 16:30:05
	Date Time: Long	2008.1.28 16.30.05 PST	2008-01-28 16:30:05 GMT–8
	Date: Short	2008.1.28	2008-01-28
	Date: Long	Pirmadienis, 2008, sausio 28	2008 m. sausio 28 d.
	Time	16:30	16:30
	Number: Positive	1 234 567,57	1 234 567,567
	Number: Negative	-1 234 567,57	–1 234 567,567
	Currency: Positive	1 234 567,57 €	1 234 567,57 €
	Currency: Negative	-1 234 567,57 €	–1 234 567,57 €
	Accounting Currency: Positive	1 234 567,57 €	1 234 567,57 €
	Accounting Currency: Negative	-1 234 567,57 €	–1 234 567,57 €
Latviešu (Latvija) lv_LV	Date Time: Medium	28.01.2008 16:30:05	2008. gada 28. janv. 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008 16:30:05 GMT-8
	Date: Medium	28.01.2008	2008. gada 28. janv.
	Date: Long	pirmdiena, 2008, 28 janvāris	2008. gada 28. janvāris
	Currency: Positive	1 234 567,57 €	1 234 567,57 €
	Currency: Negative	-1 234 567,57 €	-1 234 567,57 €
	Accounting Currency: Positive	1 234 567,57 €	1 234 567,57 €
	Accounting Currency: Negative	-1 234 567,57 €	-1 234 567,57 €
Македонски (Северна Македонија) mk_MK	Date Time: Short	28.1.2008 16:30	28.1.2008, во 16:30
	Date Time: Medium	28.1.2008 16:30:	28.1.2008, во 16:30:05
	Date Time: Long	28.1.2008 16:30:05 PST	28.1.2008, во 16:30:05 GMT-8
	Date: Long	28, јануари 2008	28 јануари 2008
	Number: Negative	(1.234.567,567)	-1.234.567,567
	Currency: Positive	Den 1.234.567,57	1.234.567,57 ден.
	Currency: Negative	-Den 1.234.567,57	-1.234.567,57 ден.
	Accounting Currency: Positive	Den 1.234.567,57	1.234.567,57 ден.
	Accounting Currency: Negative	-Den 1.234.567,57	-1.234.567,57 ден.

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
Melayu (Malaysia) ms_MY	Date Time: Short	28/01/2008 4:30 PM	28/01/2008, 4:30 PTG
	Date Time: Medium	28 Januari 2008 4:30:05 PM	28 Jan 2008, 4:30:05 PTG
	Date Time: Long	28/01/2008 4:30:05 PM PST	28/01/2008, 4:30:05 PTG GMT-8
	Date: Medium	28 Januari 2008	28 Jan 2008
	Time	4:30 PM	4:30 PTG
	Currency: Positive	RM1,234,567.57	RM 1,234,567.57
	Currency: Negative	(RM1,234,567.57)	-RM 1,234,567.57
	Accounting Currency: Positive	RM1,234,567.57	RM 1,234,567.57
	Accounting Currency: Negative	(RM1,234,567.57)	(RM 1,234,567.57)
Malti (Malta) mt_MT	Date Time: Long	28/01/2008 16:30:05 PST	28/01/2008 16:30:05 GMT-8
Nederlands (België) nl_BE	Date Time: Medium	28-jan-2008 16:30:05	28 jan. 2008 16:30:05
	Date: Medium	28-jan-2008	28 jan. 2008
	Currency: Positive	1.234.567,57 €	€ 1.234.567,57
	Currency: Negative	-1.234.567,57 €	€ -1.234.567,57
	Accounting Currency: Positive	1.234.567,57 €	€ 1.234.567,57
	Accounting Currency: Negative	-1.234.567,57 €	(€ 1.234.567,57)
Nederlands (Nederland) nl_NL	Date Time: Short	28-1-2008 16:30	28-01-2008 16:30
	Date Time: Medium	28-jan-2008 16:30:05	28 jan. 2008 16:30:05
	Date Time: Long	28-1-2008 16:30:05 PST	28-01-2008 16:30:05 PST
	Date: Short	28-1-2008	28-01-2008
	Date: Medium	28-jan-2008	28 jan. 2008
	Currency: Positive	€ 1.234.567,57	€ 1.234.567,57
	Currency: Negative	€ 1.234.567,57-	€ -1.234.567,57
	Accounting Currency: Positive	€ 1.234.567,57	€ 1.234.567,57
	Accounting Currency: Negative	€ 1.234.567,57-	(€ 1.234.567,57)
Norsk (Norge) no_NO	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	28.jan.2008 16:30:05	28. jan. 2008, 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 PST
	Date: Medium	28.jan.2008	28. jan. 2008

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Number: Negative	-1 234 567,567	–1 234 567,567
	Currency: Positive	kr 1 234 567,57	kr 1 234 567,57
	Currency: Negative	kr -1 234 567,57	kr –1 234 567,57
	Accounting Currency: Positive	kr 1 234 567,57	kr 1 234 567,57
	Accounting Currency: Negative	kr -1 234 567,57	(kr 1 234 567,57)
Polski (Polska) pl_PL	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	2008-01-28 16:30:05	28 sty 2008, 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 GMT-8
	Date: Medium	2008-01-28	28 sty 2008
	Currency: Positive	1 234 567,57 zł	1 234 567,57 zł
	Currency: Negative	-1 234 567,57 zł	-1 234 567,57 zł
	Accounting Currency: Positive	1 234 567,57 zł	1 234 567,57 zł
	Accounting Currency: Negative	-1 234 567,57 zł	(1 234 567,57 zł)
Português (Brasil) pt_BR	Date Time: Medium	28/01/2008 16:30:05	28 de jan. de 2008 16:30:05
	Date Time: Long	28/01/2008 16h30min5s PST	28/01/2008 16:30:05 GMT-8
	Date: Medium	28/01/2008	28 de jan. de 2008
	Date: Long	28 de Janeiro de 2008	28 de janeiro de 2008
	Currency: Positive	R\$ 1.234.567,57	R\$ 1.234.567,57
	Currency: Negative	-R\$ 1.234.567,57	-R\$ 1.234.567,57
	Accounting Currency: Positive	R\$ 1.234.567,57	R\$ 1.234.567,57
	Accounting Currency: Negative	-R\$ 1.234.567,57	-R\$ 1.234.567,57
Português (Portugal) pt_PT	Date Time: Short	28-01-2008 16:30	28/01/2008, 16:30
	Date Time: Medium	28/jan/2008 16:30:05	28/01/2008, 16:30:05
	Date Time: Long	28-01-2008 16:30:05 PST	28/01/2008, 16:30:05 GMT-8
	Date: Short	28-01-2008	28/01/2008
	Date: Medium	28/jan/2008	28/01/2008
	Date: Long	28 de Janeiro de 2008	28 de janeiro de 2008
	Number: Positive	1.234.567,567	1 234 567,567
	Number: Negative	-1.234.567,567	-1 234 567,567
	Currency: Positive	1.234.567,57 €	1 234 567,57 €

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Currency: Negative	-1.234.567,57 €	-1 234 567,57 €
	Accounting Currency: Positive	1.234.567,57 €	1 234 567,57 €
	Accounting Currency: Negative	-1.234.567,57 €	(1 234 567,57 €)
Română (România) ro_RO	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	28.01.2008 16:30:05	28 ian. 2008, 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 GMT-8
	Date: Medium	28.01.2008	28 ian. 2008
	Currency: Positive	1.234.567,57 LEI	1.234.567,57 RON
	Currency: Negative	-1.234.567,57 LEI	-1.234.567,57 RON
	Accounting Currency: Positive	1.234.567,57 LEI	1.234.567,57 RON
	Accounting Currency: Negative	-1.234.567,57 LEI	(1.234.567,57 RON)
Русский (Армения) ru_AM	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	28.01.2008 16:30:05	28 янв. 2008 г., 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 GMT-8
	Date: Medium	28.01.2008	28 янв. 2008 г.
	Currency: Positive	AMD 1 234 567,57	1 234 567,57 AMD
	Currency: Negative	-AMD 1 234 567,57	-1 234 567,57 AMD
	Accounting Currency: Positive	AMD 1 234 567,57	1 234 567,57 AMD
	Accounting Currency: Negative	-AMD 1 234 567,57	-1 234 567,57 AMD
Русский (Литва) ru_LT	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	28.01.2008 16:30:05	28 янв. 2008 г., 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 GMT-8
	Date: Medium	28.01.2008	28 янв. 2008 г.
	Currency: Positive	€ 1 234 567,57	1 234 567,57 €
	Currency: Negative	-€ 1 234 567,57	-1 234 567,57 €
	Accounting Currency: Positive	€ 1 234 567,57	1 234 567,57 €
	Accounting Currency: Negative	-€ 1 234 567,57	-1 234 567,57 €
Русский (Польша) ru_PL	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	28.01.2008 16:30:05	28 янв. 2008 г., 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 GMT-8

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Date: Medium	28.01.2008	28 янв. 2008 г.
	Currency: Positive	PLN 1 234 567,57	1 234 567,57 PLN
	Currency: Negative	-PLN 1 234 567,57	-1 234 567,57 PLN
	Accounting Currency: Positive	PLN 1 234 567,57	1 234 567,57 PLN
	Accounting Currency: Negative	-PLN 1 234 567,57	-1 234 567,57 PLN
Русский (Россия)	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
ru_RU	Date Time: Medium	28.01.2008 16:30:05	28 янв. 2008 г., 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 GMT-8
	Date: Medium	28.01.2008	28 янв. 2008 г.
	Currency: Positive	1 234 567,57 руб.	1 234 567,57 □
	Currency: Negative	-1 234 567,57 руб.	-1 234 567,57 □
	Accounting Currency: Positive	1 234 567,57 руб.	1 234 567,57 □
	Accounting Currency: Negative	-1 234 567,57 руб.	-1 234 567,57 □
Serbian (Latin) (Bosnia and Herzegovina)	Date Time: Short	1/28/2008 4:30 po podne	28.1.2008. 16:30
	Date Time: Medium	jan 28, 2008 4:30:05 po podne	28. 1. 2008. 16:30:05
sh_BA	Date Time: Long	1/28/2008 4:30:05 po podne GMT-8	28.1.2008. 16:30:05 GMT-8
	Date: Short	1/28/2008	28.1.2008.
	Date: Medium	jan 28, 2008	28. 1. 2008.
	Date: Long	januar 28, 2008	28. januar 2008.
	Time	4:30 po podne	16:30
Serbian (Latin) (Serbia) ¹	Locale Name	Serbian (Latin) (Serbia) ¹	Serbian (Latin) (Serbia)
sh_CS	Date Time: Short	1/28/2008 4:30 PM	28.1.2008. 16:30
	Date Time: Medium	jan 28, 2008 4:30:05 PM	28. 1. 2008. 16:30:05
	Date Time: Long	1/28/2008 4:30:05 PM GMT-8	28.1.2008. 16:30:05 GMT-8
	Date: Short	1/28/2008	28.1.2008.
	Date: Medium	jan 28, 2008	28. 1. 2008.
	Date: Long	januar 28, 2008	28. januar 2008.
Time	4:30 PM	16:30	
Montenegrin (Montenegro)	Date Time: Short	28.1.2008. 16.30	28.1.2008. 16:30

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
sh_ME	Date Time: Medium	28.01.2008. 16.30.05	28. 1. 2008. 16:30:05
	Date Time: Long	28.1.2008. 16.30.05 GMT-8	28.1.2008. 16:30:05 GMT-8
	Date: Medium	28.01.2008.	28. 1. 2008.
	Date: Long	28.01.2008.	28. januar 2008.
	Time	16.30	16:30
Montenegrin (Montenegro, USD)	Date Time: Short	28.1.2008. 16.30	28.1.2008. 16:30
	Date Time: Medium	28.01.2008. 16.30.05	28. 1. 2008. 16:30:05
sh_ME_USD	Date Time: Long	28.1.2008. 16.30.05 GMT-8	28.1.2008. 16:30:05 GMT-8
	Date: Medium	28.01.2008.	28. 1. 2008.
	Date: Long	28.01.2008.	28. januar 2008.
	Time	16.30	16:30
	Currency: Negative	(¤1,234,567.57)	-¤1,234,567.57
Slovenčina (Slovensko) sk_SK	Date Time: Short	28.1.2008 16:30	28. 1. 2008 16:30
	Date Time: Medium	28.1.2008 16:30:05	28. 1. 2008, 16:30:05
	Date Time: Long	28.1.2008 16:30:05 PST	28. 1. 2008 16:30:05 GMT-8
	Date: Short	28.1.2008	28. 1. 2008
	Date: Medium	28.1.2008	28. 1. 2008
	Date: Long	Ponedelok, 2008, januára 28	28. januára 2008
	Currency: Positive	1 234 567,57 €	1 234 567,57 €
	Currency: Negative	-1 234 567,57 €	-1 234 567,57 €
	Accounting Currency: Positive	1 234 567,57 €	1 234 567,57 €
	Accounting Currency: Negative	-1 234 567,57 €	(1 234 567,57 €)
Slovenščina (Slovenija) sl_SI	Date Time: Short	28.1.2008 16:30	28. 01. 2008, 16:30
	Date Time: Medium	28.1.2008 16:30:05	28. jan. 2008, 16:30:05
	Date Time: Long	28.1.2008 16:30:05 PST	28. 01. 2008, 16:30:05 GMT-8
	Date: Short	28.1.2008	28. 01. 2008
	Date: Medium	28.1.2008	28. jan. 2008
	Number: Negative	-1.234.567,567	-1.234.567,567
	Currency: Positive	€ 1.234.567,57	1.234.567,57 €
	Currency: Negative	-€ 1.234.567,57	-1.234.567,57 €

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Accounting Currency: Positive	€ 1.234.567,57	1.234.567,57 €
	Accounting Currency: Negative	-€ 1.234.567,57	(1.234.567,57 €)
Samoan (United States) sm_US	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 4:30 PM
	Date Time: Medium	Jan 28, 2008 4:30:05 PM	Jan 28, 2008, 4:30:05 PM
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 4:30:05 PM PST
	Currency: Positive	USD 1,234,567.57	\$1,234,567.57
	Currency: Negative	-USD 1,234,567.57	-\$1,234,567.57
	Accounting Currency: Positive	USD 1,234,567.57	\$1,234,567.57
	Accounting Currency: Negative	-USD 1,234,567.57	(\$1,234,567.57)
Samoan (Samoa) sm_WS	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 4:30 PM
	Date Time: Medium	Jan 28, 2008 4:30:05 PM	Jan 28, 2008, 4:30:05 PM
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 4:30:05 PM PST
	Currency: Positive	WST 1,234,567.57	WST 1,234,567.57
	Currency: Negative	-WST 1,234,567.57	-WST 1,234,567.57
	Accounting Currency: Positive	WST 1,234,567.57	WST 1,234,567.57
	Accounting Currency: Negative	-WST 1,234,567.57	(WST 1,234,567.57)
Shqip (Shqipëri) sq_AL	Date Time: Short	2008-01-28 4.30.MD	28.1.2008, 4:30 e pasdites
	Date Time: Medium	2008-01-28 4:30:05.MD	28 jan 2008, 4:30:05 e pasdites
	Date Time: Long	2008-01-28 4.30.05.MD PST	28.1.2008, 4:30:05 e pasdites, GMT-8
	Date: Short	2008-01-28	28.1.2008
	Date: Medium	2008-01-28	28 jan 2008
	Date: Long	2008-01-28	28 janar 2008
	Time	4.30.MD	4:30 e pasdites
	Number: Positive	1.234.567,567	1 234 567,567
	Number: Negative	-1.234.567,567	-1 234 567,567
	Currency: Positive	Lek1.234.567,57	1 234 567,57 Lekë
	Currency: Negative	-Lek1.234.567,57	-1 234 567,57 Lekë
	Accounting Currency: Positive	Lek1.234.567,57	1 234 567,57 Lekë
	Accounting Currency: Negative	-Lek1.234.567,57	(1 234 567,57 Lekë)

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
Serbian (Cyrillic) (Bosnia and Herzegovina) sr_BA	Date Time: Short	2008-01-28 16:30	28.1.2008. 16:30
	Date Time: Medium	2008-01-28 16:30:05	28. 1. 2008. 16:30:05
	Date Time: Long	2008-01-28 16.30.05 PST	28.1.2008. 16:30:05 GMT-8
	Date: Short	2008-01-28	28.1.2008.
	Date: Medium	2008-01-28	28. 1. 2008.
	Currency: Positive	KM. 1.234.567,57	1.234.567,57 KM
	Currency: Negative	-KM. 1.234.567,57	-1.234.567,57 KM
	Accounting Currency: Positive	KM. 1.234.567,57	1.234.567,57 KM
	Accounting Currency: Negative	-KM. 1.234.567,57	(1.234.567,57 KM)
Serbian (Cyrillic) (Serbia) ¹ sr_CS	Locale Name	Serbian (Cyrillic) (Serbia) ¹	Serbian (Cyrillic) (Serbia)
	Date Time: Short	28.1.2008. 16.30	28.1.2008. 16:30
	Date Time: Medium	28.01.2008. 16.30.05	28. 1. 2008. 16:30:05
	Date Time: Long	28.1.2008. 16.30.05 PST	28.1.2008. 16:30:05 GMT-8
	Date: Medium	28.01.2008.	28. 1. 2008.
	Date: Long	28.01.2008.	28. јануар 2008.
	Time	16.30	16:30
	Currency: Positive	CSD 1.234.567,57	1.234.567,57 CSD
	Currency: Negative	-CSD 1.234.567,57	-1.234.567,57 CSD
	Accounting Currency: Positive	CSD 1.234.567,57	1.234.567,57 CSD
Accounting Currency: Negative	-CSD 1.234.567,57	(1.234.567,57 CSD)	
Српски (Србија) sr_RS	Date Time: Short	28.1.2008. 16.30	28.1.2008. 16:30
	Date Time: Medium	28.01.2008. 16.30.05	28. 1. 2008. 16:30:05
	Date Time: Long	28.1.2008. 16.30.05 PST	28.1.2008. 16:30:05 GMT-8
	Date: Medium	28.01.2008.	28. 1. 2008.
	Date: Long	28.01.2008.	28. јануар 2008.
	Time	16.30	16:30
	Currency: Positive	дин. 1.234.567,57	1.234.567,57 RSD
	Currency: Negative	-дин. 1.234.567,57	-1.234.567,57 RSD
	Accounting Currency: Positive	дин. 1.234.567,57	1.234.567,57 RSD

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Accounting Currency: Negative	-дин. 1.234.567,57	(1.234.567,57 RSD)
Svenska (Sverige) sv_SE	Date Time: Medium	2008-jan-28 16:30:05	28 jan. 2008 16:30:05
	Date Time: Long	2008-01-28 16:30:05 PST	2008-01-28 16:30:05 GMT-8
	Date: Medium	2008-jan-28	28 jan. 2008
	Date: Long	den 28 januari 2008	28 januari 2008
	Number: Negative	-1 234 567,567	-1 234 567,567
	Currency: Positive	1 234 567,57 kr	1 234 567,57 kr
	Currency: Negative	-1 234 567,57 kr	-1 234 567,57 kr
	Accounting Currency: Positive	1 234 567,57 kr	1 234 567,57 kr
	Accounting Currency: Negative	-1 234 567,57 kr	-1 234 567,57 kr
() th_TH	Date Time: Short	28/1/2551, 16:30 น.	28/1/2551 16:30
	Date Time: Medium	28 ม.ค. 2551, 16:30:05	28 ม.ค. 2551 16:30:05
	Date Time: Long	28/1/2551, 16 นาฬิกา 30 นาที	28/1/2551 16 นาฬิกา 30 นาที 05 วินาที GMT-8
	Time	16:30 น.	16:30
	Currency: Negative	฿-1,234,567.57	-฿1,234,567.57
	Accounting Currency: Negative	฿-1,234,567.57	(฿1,234,567.57)
Tagalog (Pilipinas) tl_PH	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 4:30 PM
	Date Time: Medium	Jan 28, 2008 4:30:05 PM	Ene 28, 2008, 4:30:05 PM
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 4:30:05 PM GMT-8
	Date: Medium	Jan 28, 2008	Ene 28, 2008
	Date: Long	January 28, 2008	Enero 28, 2008
	Currency: Positive	PHP 1,234,567.57	1,234,567.57
	Currency: Negative	-PHP 1,234,567.57	- 1,234,567.57
	Accounting Currency: Positive	PHP 1,234,567.57	1,234,567.57
	Accounting Currency: Negative	-PHP 1,234,567.57	(1,234,567.57)
Türkçe (Türkiye) tr_TR	Date Time: Medium	28.Oca.2008 16:30:05	28 Oca 2008 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008 16:30:05 GMT-8
	Date: Medium	28.Oca.2008	28 Oca 2008
	Date: Long	28 Ocak 2008 Pazartesi	28 Ocak 2008
	Currency: Positive	1.234.567,57 TL	1.234.567,57

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Currency: Negative	-1.234.567,57 TL	- 1.234.567,57
	Accounting Currency: Positive	1.234.567,57 TL	1.234.567,57
	Accounting Currency: Negative	-1.234.567,57 TL	- 1.234.567,57
Українська (Україна) uk_UA	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	28 січ. 2008 16:30:05	28 січ. 2008 р., 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 GMT-8
	Date: Medium	28 січ. 2008	28 січ. 2008 р.
	Date: Long	28 січня 2008	28 січня 2008 р.
	Currency: Positive	1 234 567,57 грн.	1 234 567,57
	Currency: Negative	-1 234 567,57 грн.	-1 234 567,57
	Accounting Currency: Positive	1 234 567,57 грн.	1 234 567,57
	Accounting Currency: Negative	-1 234 567,57 грн.	-1 234 567,57
Ti ng Vi t (Vi t Nam) vi_VN	Date Time: Short	16:30 28/01/2008	16:30, 28/01/2008
	Date Time: Medium	16:30:05 28-01-2008	16:30:05, 28 thg 1, 2008
	Date Time: Long	16:30:05 PST 28/01/2008	16:30:05 PST, 28/01/2008
	Date: Medium	28-01-2008	28 thg 1, 2008
	Date: Long	Ngày 28 tháng 1 năm 2008	28 tháng 1, 2008
	Currency: Positive	1.234.567,57 đ	1.234.567,57
	Currency: Negative	-1.234.567,57 đ	-1.234.567,57
	Accounting Currency: Positive	1.234.567,57 đ	1.234.567,57
	Accounting Currency: Negative	-1.234.567,57 đ	-1.234.567,57
zh_CN	Date Time: Short	2008-1-28 下午4:30	2008/1/28 16:30
	Date Time: Medium	2008-1-28 16:30:05	2008年1月28日 16:30:05
	Date Time: Long	2008-1-28 下午04时30分05秒	2008/1/28 GMT-8 16:30:05
	Date: Short	2008-1-28	2008/1/28
	Date: Medium	2008-1-28	2008年1月28日
	Time	下午4:30	16:30
	Currency: Positive	¥1,234,567.57	¥1,234,567.57
	Currency: Negative	-¥1,234,567.57	-¥1,234,567.57
	Accounting Currency: Positive	¥1,234,567.57	¥1,234,567.57

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
CNH zh_CN_CNH	Accounting Currency: Negative	- ¥1,234,567.57	(¥1,234,567.57)
	Date Time: Short	2008-1-28 下午4:30	2008/1/28 16:30
	Date Time: Medium	2008-1-28 16:30:05	2008年1月28日 16:30:05
	Date Time: Long	2008-1-28 下午04时30分05秒	2008/1/28 GMT-8 16:30:05
	Date: Short	2008-1-28	2008/1/28
	Date: Medium	2008-1-28	2008年1月28日
	Time	下午4:30	16:30
	Currency: Positive	CNH1,234,567.57	CNH 1,234,567.57
	Currency: Negative	-CNH1,234,567.57	-CNH 1,234,567.57
	Accounting Currency: Positive	CNH1,234,567.57	CNH 1,234,567.57
Accounting Currency: Negative	-CNH1,234,567.57	(CNH 1,234,567.57)	
zh_CN_PINYIN	Date Time: Short	2008-1-28 下午4:30	2008/1/28 16:30
	Date Time: Medium	2008-1-28 16:30:05	2008年1月28日 16:30:05
	Date Time: Long	2008-1-28 下午04时30分05秒	2008/1/28 GMT-8 16:30:05
	Date: Short	2008-1-28	2008/1/28
	Date: Medium	2008-1-28	2008年1月28日
	Time	下午4:30	16:30
	Currency: Positive	¥1,234,567.57	¥1,234,567.57
	Currency: Negative	-¥1,234,567.57	-¥1,234,567.57
	Accounting Currency: Positive	¥1,234,567.57	¥1,234,567.57
	Accounting Currency: Negative	-¥1,234,567.57	(¥1,234,567.57)
中文 (中国, 笔画顺序) zh_CN_STROKE	Date Time: Short	2008-1-28 下午4:30	2008/1/28 16:30
	Date Time: Medium	2008-1-28 16:30:05	2008年1月28日 16:30:05
	Date Time: Long	2008-1-28 下午04时30分05秒	2008/1/28 GMT-8 16:30:05
	Date: Short	2008-1-28	2008/1/28
	Date: Medium	2008-1-28	2008年1月28日
	Time	下午4:30	16:30
	Currency: Positive	¥1,234,567.57	¥1,234,567.57
	Currency: Negative	-¥1,234,567.57	-¥1,234,567.57
	Accounting Currency: Positive	¥1,234,567.57	¥1,234,567.57
	Accounting Currency: Negative	-¥1,234,567.57	(¥1,234,567.57)

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
zh_HK	Accounting Currency: Negative	- ¥1,234,567.57	(¥1,234,567.57)
	Date Time: Short	2008 1 28 4:30	28/1/2008 4:30
	Date Time: Medium	2008 1 28 04:30:05	2008 1 28 4:30:05
	Date Time: Long	2008 1 28 04 30 05	28/1/2008 4:30:05 [PST]
	Date: Short	2008 1 28	28/1/2008
	Date: Long	2008 01 28	2008 1 28
	Currency: Negative	(HK\$1,234,567.57)	-HK\$1,234,567.57
() zh_HK_STROKE	Date Time: Short	2008 1 28 4:30	28/1/2008 4:30
	Date Time: Medium	2008 1 28 04:30:05	2008 1 28 4:30:05
	Date Time: Long	2008 1 28 04 30 05	28/1/2008 4:30:05 [PST]
	Date: Short	2008 1 28	28/1/2008
	Date: Long	2008 01 28	2008 1 28
	Currency: Negative	(HK\$1,234,567.57)	-HK\$1,234,567.57
	zh_MY	Date Time: Short	2008-1-28 4:30
Date Time: Medium		2008-1-28 16:30:05	2008 1 28 4:30:05
Date Time: Long		2008-1-28 04 30 05	2008/1/28 GMT-8 4:30:05
Date: Short		2008-1-28	2008/1/28
Date: Medium		2008-1-28	2008 1 28
Currency: Positive		MYR 1,234,567.57	MYR 1,234,567.57
Currency: Negative		-MYR 1,234,567.57	-MYR 1,234,567.57
Accounting Currency: Positive		MYR 1,234,567.57	MYR 1,234,567.57
Accounting Currency: Negative		-MYR 1,234,567.57	(MYR 1,234,567.57)
zh_SG	Date Time: Short	28/01/2008 04:30	28/01/2008 4:30
	Date Time: Medium	28- -2008 04:30	2008 1 28 4:30:05
	Date Time: Long	28/01/2008 04:30:05	28/01/2008 GMT-8 4:30:05
	Date: Medium	28- -2008	2008 1 28
	Date: Long	28 2008	2008 1 28
	Time	04:30	4:30
	Currency: Positive	S\$1,234,567.57	\$1,234,567.57
Currency: Negative	-S\$1,234,567.57	-\$1,234,567.57	

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
zh_TW	Accounting Currency: Positive	\$S\$1,234,567.57	\$1,234,567.57
	Accounting Currency: Negative	-\$S\$1,234,567.57	(\$1,234,567.57)
	Date Time: Short	2008/1/28 下午 4:30	2008/1/28 下午4:30
	Date Time: Medium	2008/1/28 下午 04:30:05	2008年1月28日 下午4:30:05
	Date Time: Long	2008/1/28 下午04時30分05秒	2008/1/28 下午4:30:05 [PST]
	Date: Medium	2008/1/28	2008年1月28日
	Time	下午 4:30	下午4:30
	Currency: Positive	NTS\$1,234,567.57	\$1,234,567.57
	Currency: Negative	-NTS\$1,234,567.57	-\$1,234,567.57
	Accounting Currency: Positive	NTS\$1,234,567.57	\$1,234,567.57
Accounting Currency: Negative	-NTS\$1,234,567.57	(\$1,234,567.57)	
中文 (台灣， 筆劃順序) zh_TW_STROKE	Date Time: Short	2008/1/28 下午 4:30	2008/1/28 下午4:30
	Date Time: Medium	2008/1/28 下午 04:30:05	2008年1月28日 下午4:30:05
	Date Time: Long	2008/1/28 下午04時30分05秒	2008/1/28 下午4:30:05 [PST]
	Date: Medium	2008/1/28	2008年1月28日
	Time	下午 4:30	下午4:30
	Currency: Positive	NTS\$1,234,567.57	\$1,234,567.57
	Currency: Negative	-NTS\$1,234,567.57	-\$1,234,567.57
	Accounting Currency: Positive	NTS\$1,234,567.57	\$1,234,567.57
	Accounting Currency: Negative	-NTS\$1,234,567.57	(\$1,234,567.57)

¹ The CSD currency is only available in single currency orgs and orgs that activated multiple currencies when CSD was the corporate currency. It represents the old Serbian Dinar used in Serbia and Montenegro from 2003 to 2006. Because it's no longer a valid ISO currency code, it can be incompatible with other systems. If your org uses this currency, we recommend moving to the current Serbian Dinar currency, RSD. The corresponding locale is Serbian (Serbia) with the sr_RS locale code.

Changes to Language-Only Locales

Language-only locales do not include a currency and are no longer recommended. If your users have selected a language-only locale, we recommend they switch to a Salesforce supported locale.

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Date Time: Short	28/01/2008 04:30	// , :

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
ar	Date Time: Medium	28/01/2008 04:30:05	/ / , : :
	Date Time: Long	28/01/2008 PST 04:30:05	/ / , : : -
	Date: Short	28/01/2008	/ /
	Date: Medium	28/01/2008	/ /
	Date: Long	28 , 2008	
	Time	04:30	:
	Number: Positive	1,234,567.567	
	Number: Negative	1,234,567.567-	-
	Currency: Positive	¤ 1,234,567.57	¤
	Currency: Negative	¤ 1,234,567.57-	- ¤
	Accounting Currency: Positive	¤ 1,234,567.57	¤
	Accounting Currency: Negative	¤ 1,234,567.57-	- ¤
Български bg	Date Time: Short	28.01.2008 16:30	28.01.2008 г., 16:30 ч.
	Date Time: Medium	28.01.2008 16:30:05	28.01.2008 г., 16:30:05 ч.
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008 г., 16:30:05 ч. Гринуич-8
	Date: Short	28.01.2008	28.01.2008 г.
	Date: Medium	28.01.2008	28.01.2008 г.
	Date: Long	28 Януари 2008	28 януари 2008 г.
	Time	16:30	16:30 ч.
	Currency: Positive	¤ 1 234 567,57	1234567,57 ¤
	Currency: Negative	-¤ 1 234 567,57	-1234567,57 ¤
	Accounting Currency: Positive	¤ 1 234 567,57	1234567,57 ¤
	Accounting Currency: Negative	-¤ 1 234 567,57	(1234567,57 ¤)
	Català ca	Date Time: Short	28/01/2008 16:30
Date Time: Medium		28/01/2008 16:30:05	28 de gen. 2008, 16:30:05
Date Time: Long		28/01/2008 16:30:05 PST	28/1/2008 16:30:05 GMT-8
Date: Short		28/01/2008	28/1/2008
Date: Medium		28/01/2008	28 de gen. 2008
Date: Long		28 / de gener / 2008	28 de gener de 2008
Currency: Positive		¤ 1.234.567,57	1.234.567,57 XXX

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 XXX
	Accounting Currency: Positive	¤ 1.234.567,57	1.234.567,57 XXX
	Accounting Currency: Negative	-¤ 1.234.567,57	(1.234.567,57 XXX)
Cac	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 16:30
caC	Date Time: Medium	Jan 28, 2008 4:30:05 PM	Jan 28, 2008, 16:30:05
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 16:30:05 PST
	Time	4:30 PM	16:30
	Currency: Positive	¤ 1,234,567.57	\$1,234,567.57
	Currency: Negative	-¤ 1,234,567.57	-\$1,234,567.57
	Accounting Currency: Positive	¤ 1,234,567.57	\$1,234,567.57
	Accounting Currency: Negative	-¤ 1,234,567.57	(\$1,234,567.57)
Cak	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 16:30
caK	Date Time: Medium	Jan 28, 2008 4:30:05 PM	Jan 28, 2008, 16:30:05
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 16:30:05 PST
	Time	4:30 PM	16:30
	Currency: Positive	¤ 1,234,567.57	\$1,234,567.57
	Currency: Negative	-¤ 1,234,567.57	-\$1,234,567.57
	Accounting Currency: Positive	¤ 1,234,567.57	\$1,234,567.57
	Accounting Currency: Negative	-¤ 1,234,567.57	(\$1,234,567.57)
Čeština	Date Time: Short	28.1.2008 16:30	28.01.2008 16:30
cs	Date Time: Medium	28.1.2008 16:30:05	28. 1. 2008 16:30:05
	Date Time: Long	28.1.2008 16:30:05 PST	28.01.2008 16:30:05 PST
	Date: Short	28.1.2008	28.01.2008
	Date: Medium	28.1.2008	28. 1. 2008
	Currency: Positive	¤ 1 234 567,57	1 234 567,57 XXX
	Currency: Negative	-¤ 1 234 567,57	-1 234 567,57 XXX
	Accounting Currency: Positive	¤ 1 234 567,57	1 234 567,57 XXX
	Accounting Currency: Negative	-¤ 1 234 567,57	-1 234 567,57 XXX
Dansk	Date Time: Short	28-01-2008 16:30	28.01.2008 16:30
da	Date Time: Medium	28-01-2008 16:30:05	28. jan. 2008 16:30:05

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Date Time: Long	28-01-2008 16:30:05 PST	28.01.2008 16.30.05 GMT-8
	Date: Short	28-01-2008	28.01.2008
	Date: Medium	28-01-2008	28. jan. 2008
	Time	16:30	16.30
	Currency: Positive	¤ 1.234.567,57	1.234.567,57 ¤
	Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 ¤
	Accounting Currency: Positive	¤ 1.234.567,57	1.234.567,57 ¤
	Accounting Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 ¤
Deutsch de	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	28.01.2008 16:30:05	28.01.2008, 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 GMT-8
	Currency: Positive	¤ 1.234.567,57	1.234.567,57 XXX
	Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 XXX
	Accounting Currency: Positive	¤ 1.234.567,57	1.234.567,57 XXX
	Accounting Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 XXX
Ελληνικά el	Date Time: Short	28/1/2008 4:30 μμ	28/1/2008, 4:30 μ.μ.
	Date Time: Medium	28 Ιαν 2008 4:30:05 μμ	28 Ιαν 2008, 4:30:05 μ.μ.
	Date Time: Long	28/1/2008 4:30:05 μμ PST	28/1/2008, 4:30:05 μ.μ. GMT-8
	Time	4:30 μμ	4:30 μ.μ.
	Currency: Positive	¤ 1.234.567,57	1.234.567,57 ¤
	Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 ¤
	Accounting Currency: Positive	¤ 1.234.567,57	1.234.567,57 ¤
Accounting Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 ¤	
Español es	Date Time: Short	28/01/2008 16:30	28/1/2008, 16:30
	Date Time: Medium	28-ene-2008 16:30:05	28 ene 2008, 16:30:05
	Date Time: Long	28/01/2008 16:30:05 PST	28/1/2008, 16:30:05 GMT-8
	Date: Short	28/01/2008	28/1/2008
	Date: Medium	28-ene-2008	28 ene 2008
	Currency: Positive	¤1.234.567,57	1.234.567,57 ¤
	Currency: Negative	(¤1.234.567,57)	-1.234.567,57 ¤

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Accounting Currency: Positive	¤1.234.567,57	1.234.567,57 ¤
	Accounting Currency: Negative	(¤1.234.567,57)	-1.234.567,57 ¤
Eesti et	Date Time: Medium	28.01.2008 16:30:05	28. jaan 2008 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008 16:30:05 GMT –8
	Date: Medium	28.01.2008	28. jaan 2008
	Date: Long	esmaspäev, 28. jaanuar 2008. a	28. jaanuar 2008
	Number: Negative	-1 234 567,567	–1 234 567,567
	Currency: Positive	¤ 1 234 567,57	1 234 567,57 ¤
	Currency: Negative	-¤ 1 234 567,57	–1 234 567,57 ¤
	Accounting Currency: Positive	¤ 1 234 567,57	1 234 567,57 ¤
	Accounting Currency: Negative	-¤ 1 234 567,57	(1 234 567,57 ¤)
Suomi fi	Date Time: Short	28.1.2008 16:30	28.1.2008 16.30
	Date Time: Medium	28.1.2008 16:30:05	28.1.2008 klo 16.30.05
	Date Time: Long	28.1.2008 klo 16.30.05	28.1.2008 16.30.05 UTC-8
	Time	16:30	16.30
	Number: Negative	-1 234 567,567	–1 234 567,567
	Currency: Positive	¤ 1 234 567,57	1 234 567,57 XXX
	Currency: Negative	-¤ 1 234 567,57	–1 234 567,57 XXX
	Accounting Currency: Positive	¤ 1 234 567,57	1 234 567,57 XXX
	Accounting Currency: Negative	-¤ 1 234 567,57	–1 234 567,57 XXX
Français fr	Date Time: Medium	28 janv. 2008 16:30:05	28 janv. 2008, 16:30:05
	Date Time: Long	28/01/2008 16:30:05 PST	28/01/2008 16:30:05 UTC–8
	Number: Positive	1 234 567,567	1 234 567,567
	Number: Negative	-1 234 567,567	-1 234 567,567
	Currency: Positive	1 234 567,57 ¤	1 234 567,57 ¤
	Currency: Negative	-1 234 567,57 ¤	-1 234 567,57 ¤
	Accounting Currency: Positive	1 234 567,57 ¤	1 234 567,57 ¤
	Accounting Currency: Negative	-1 234 567,57 ¤	(1 234 567,57 ¤)
Gaeilge ga	Date Time: Short	2008/01/28 16:30	28/01/2008 16:30
	Date Time: Medium	2008 Ean 28 16:30:05	28 Ean 2008 16:30:05

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Date Time: Long	2008/01/28 16:30:05 ACAC	28/01/2008 16:30:05 ACAC
	Date: Short	2008/01/28	28/01/2008
	Date: Medium	2008 Ean 28	28 Ean 2008
	Date: Long	2008 Eanáir 28	28 Eanáir 2008
	Currency: Positive	¤ 1,234,567.57	XXX 1,234,567.57
	Currency: Negative	-¤ 1,234,567.57	-XXX 1,234,567.57
	Accounting Currency: Positive	¤ 1,234,567.57	XXX 1,234,567.57
	Accounting Currency: Negative	-¤ 1,234,567.57	(XXX 1,234,567.57)
Hmong hmn	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 16:30
	Date Time: Medium	Jan 28, 2008 4:30:05 PM	Jan 28, 2008, 16:30:05
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 16:30:05 PST
	Time	4:30 PM	16:30
	Currency: Positive	¤ 1,234,567.57	\$1,234,567.57
	Currency: Negative	-¤ 1,234,567.57	-\$1,234,567.57
	Accounting Currency: Positive	¤ 1,234,567.57	\$1,234,567.57
	Accounting Currency: Negative	-¤ 1,234,567.57	(\$1,234,567.57)
Hrvatski hr	Date Time: Short	2008.01.28 16:30	28. 01. 2008. 16:30
	Date Time: Medium	2008.01.28 16:30:05	28. sij 2008. 16:30:05
	Date Time: Long	2008.01.28 16:30:05 PST	28. 01. 2008. 16:30:05 GMT -8
	Date: Short	2008.01.28	28. 01. 2008.
	Date: Medium	2008.01.28	28. sij 2008.
	Date: Long	2008. siječnja 28	28. siječnja 2008.
	Number: Negative	-1.234.567,567	–1.234.567,567
	Currency: Positive	¤ 1.234.567,57	1.234.567,57 XXX
	Currency: Negative	-¤ 1.234.567,57	–1.234.567,57 XXX
	Accounting Currency: Positive	¤ 1.234.567,57	1.234.567,57 XXX
	Accounting Currency: Negative	-¤ 1.234.567,57	–1.234.567,57 XXX
Haitian Creole ht	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 16:30
	Date Time: Medium	Jan 28, 2008 4:30:05 PM	Jan 28, 2008, 16:30:05
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 16:30:05 PST

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Time	4:30 PM	16:30
	Currency: Positive	¤ 1,234,567.57	\$1,234,567.57
	Currency: Negative	-¤ 1,234,567.57	-\$1,234,567.57
	Accounting Currency: Positive	¤ 1,234,567.57	\$1,234,567.57
	Accounting Currency: Negative	-¤ 1,234,567.57	(\$1,234,567.57)
Magyar hu	Date Time: Short	2008.01.28. 16:30	2008. 01. 28. 16:30
	Date Time: Medium	2008.01.28. 16:30:05	2008. jan. 28. 16:30:05
	Date Time: Long	2008.01.28. 16:30:05 PST	2008. 01. 28. 16:30:05 GMT-8
	Date: Short	2008.01.28.	2008. 01. 28.
	Date: Medium	2008.01.28.	2008. jan. 28.
	Currency: Positive	¤ 1 234 567,57	1 234 567,57 ¤
	Currency: Negative	-¤ 1 234 567,57	-1 234 567,57 ¤
	Accounting Currency: Positive	¤ 1 234 567,57	1 234 567,57 ¤
	Accounting Currency: Negative	-¤ 1 234 567,57	-1 234 567,57 ¤
Indonesia in	Date Time: Short	2008/01/28 16:30	28/01/2008 16.30
	Date Time: Medium	2008 Jan 28 16:30:05	28 Jan 2008 16.30.05
	Date Time: Long	2008/01/28 16:30:05 PST	28/01/2008 16.30.05 PST
	Date: Short	2008/01/28	28/01/2008
	Date: Medium	2008 Jan 28	28 Jan 2008
	Date: Long	2008 Januari 28	28 Januari 2008
	Time	16:30	16.30
	Currency: Positive	¤1.234.567,57	XXX 1.234.567,57
	Currency: Negative	-¤1.234.567,57	-XXX 1.234.567,57
	Accounting Currency: Positive	¤1.234.567,57	XXX 1.234.567,57
	Accounting Currency: Negative	-¤1.234.567,57	-XXX 1.234.567,57
Íslenska is	Date Time: Short	28.1.2008 16:30	28.1.2008, 16:30
	Date Time: Medium	28.1.2008 16:30:05	28. jan. 2008, 16:30:05
	Date Time: Long	28.1.2008 16:30:05 PST	28.1.2008, 16:30:05 GMT-8
	Date: Medium	28.1.2008	28. jan. 2008
	Currency: Positive	¤ 1.234.567,57	1.234.567,57 ¤

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 ¤
	Accounting Currency: Positive	¤ 1.234.567,57	1.234.567,57 ¤
	Accounting Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 ¤
Italiano it	Date Time: Short	28/01/2008 16.30	28/01/2008, 16:30
	Date Time: Medium	28-gen-2008 16.30.05	28 gen 2008, 16:30:05
	Date Time: Long	28/01/2008 16.30.05 PST	28/01/2008, 16:30:05 GMT-8
	Date: Medium	28-gen-2008	28 gen 2008
	Time	16.30	16:30
	Currency: Positive	¤ 1.234.567,57	1.234.567,57 ¤
	Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 ¤
	Accounting Currency: Positive	¤ 1.234.567,57	1.234.567,57 ¤
	Accounting Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 ¤
	Date Time: Short	16:30 28/01/2008	28.1.2008, 16:30
iw	Date Time: Medium	16:30:05 28/01/2008	28 2008, 16:30:05
	Date Time: Long	16:30:05 PST 28/01/2008	28.1.2008, 16:30:05 GMT-8
	Date: Short	28/01/2008	28.1.2008
	Date: Medium	28/01/2008	28 2008
	Date: Long	28 2008	28 2008
	Number: Negative	-1,234,567.567	-1,234,567.567
	Currency: Positive	¤ 1,234,567.57	1,234,567.57 ¤
	Currency: Negative	-¤ 1,234,567.57	-1,234,567.57 ¤
	Accounting Currency: Positive	¤ 1,234,567.57	1,234,567.57 ¤
	Accounting Currency: Negative	-¤ 1,234,567.57	-1,234,567.57 ¤
	Date Time: Long	2008/01/28 16:30:05 PST	2008/01/28 16:30:05 GMT-8
ja	Date: Long	2008/01/28	2008年1月28日
	Currency: Positive	¤ 1,234,567.57	XXX 1,234,567.57
	Currency: Negative	-¤ 1,234,567.57	-XXX 1,234,567.57
	Accounting Currency: Positive	¤ 1,234,567.57	XXX 1,234,567.57
	Accounting Currency: Negative	-¤ 1,234,567.57	(XXX 1,234,567.57)
	Date Time: Short	2008. 1. 28 오후 4:30	2008. 1. 28. 오후 4:30

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
ko	Date Time: Medium	2008. 1. 28 오후 4:30:05	2008. 1. 28. 오후 4:30:05
	Date Time: Long	2008. 1. 28 오후 4시 30분 05초	2008. 1. 28. 오후 4시 30분 5초 GMT-8
	Date: Short	2008. 1. 28	2008. 1. 28.
	Date: Medium	2008. 1. 28	2008. 1. 28.
	Date: Long	2008년 1월 28일 (월)	2008년 1월 28일
	Currency: Positive	₩ 1,234,567.57	₩1,234,567.57
	Currency: Negative	-₩ 1,234,567.57	-₩1,234,567.57
	Accounting Currency: Positive	₩ 1,234,567.57	₩1,234,567.57
	Accounting Currency: Negative	-₩ 1,234,567.57	(₩1,234,567.57)
Lietuvių lt	Date Time: Short	2008.1.28 16.30	2008-01-28 16:30
	Date Time: Medium	2008-01-28 16.30.05	2008-01-28 16:30:05
	Date Time: Long	2008.1.28 16.30.05 PST	2008-01-28 16:30:05 GMT-8
	Date: Short	2008.1.28	2008-01-28
	Date: Long	Pirmadienis, 2008, sausio 28	2008 m. sausio 28 d.
	Time	16.30	16:30
	Number: Negative	-1 234 567,567	-1 234 567,567
	Currency: Positive	€ 1 234 567,57	1 234 567,57 €
	Currency: Negative	-€ 1 234 567,57	-1 234 567,57 €
	Accounting Currency: Positive	€ 1 234 567,57	1 234 567,57 €
	Accounting Currency: Negative	-€ 1 234 567,57	-1 234 567,57 €
	Latviešu lv	Date Time: Short	2008.28.1 16:30
Date Time: Medium		2008.28.1 16:30:05	2008. gada 28. janv. 16:30:05
Date Time: Long		2008.28.1 16:30:05 PST	28.01.2008 16:30:05 GMT-8
Date: Short		2008.28.1	28.01.2008
Date: Medium		2008.28.1	2008. gada 28. janv.
Date: Long		pirmdiena, 2008, 28 janvāris	2008. gada 28. janvāris
Currency: Positive		€ 1 234 567,57	1 234 567,57 €
Currency: Negative		-€ 1 234 567,57	-1 234 567,57 €
Accounting Currency: Positive		€ 1 234 567,57	1 234 567,57 €

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Accounting Currency: Negative	-¤ 1 234 567,57	-1 234 567,57 ¤
Македонски и mk	Date Time: Short	28.1.2008 16:30	28.1.2008, во 16:30
	Date Time: Medium	28.1.2008 16:30:	28.1.2008, во 16:30:05
	Date Time: Long	28.1.2008 16:30:05 PST	28.1.2008, во 16:30:05 GMT-8
	Date: Long	28, јануари 2008	28 јануари 2008
	Currency: Positive	¤ 1.234.567,57	1.234.567,57 ¤
	Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 ¤
	Accounting Currency: Positive	¤ 1.234.567,57	1.234.567,57 ¤
	Accounting Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 ¤
Melayu ms	Date Time: Short	2008/01/28 16:30	28/01/2008, 4:30 PTG
	Date Time: Medium	2008 Jan 28 16:30:05	28 Jan 2008, 4:30:05 PTG
	Date Time: Long	2008/01/28 16:30:05 PST	28/01/2008, 4:30:05 PTG GMT-8
	Date: Short	2008/01/28	28/01/2008
	Date: Medium	2008 Jan 28	28 Jan 2008
	Date: Long	2008 Januari 28	28 Januari 2008
	Time	16:30	4:30 PTG
	Currency: Positive	¤ 1,234,567.57	¤1,234,567.57
	Currency: Negative	-¤ 1,234,567.57	-¤1,234,567.57
	Accounting Currency: Positive	¤ 1,234,567.57	¤1,234,567.57
	Accounting Currency: Negative	-¤ 1,234,567.57	(¤1,234,567.57)
Malti mt	Date Time: Long	28/01/2008 16:30:05 PST	28/01/2008 16:30:05 GMT-8
	Currency: Positive	¤ 1,234,567.57	¤1,234,567.57
	Currency: Negative	-¤ 1,234,567.57	-¤1,234,567.57
	Accounting Currency: Positive	¤ 1,234,567.57	¤1,234,567.57
	Accounting Currency: Negative	-¤ 1,234,567.57	-¤1,234,567.57
Nederlands nl	Date Time: Short	28-1-2008 16:30	28-01-2008 16:30
	Date Time: Medium	28-jan-2008 16:30:05	28 jan. 2008 16:30:05
	Date Time: Long	28-1-2008 16:30:05 PST	28-01-2008 16:30:05 PST
	Date: Short	28-1-2008	28-01-2008
	Date: Medium	28-jan-2008	28 jan. 2008

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Currency: Positive	¤ 1.234.567,57	XXX 1.234.567,57
	Currency: Negative	-¤ 1.234.567,57	XXX -1.234.567,57
	Accounting Currency: Positive	¤ 1.234.567,57	XXX 1.234.567,57
	Accounting Currency: Negative	-¤ 1.234.567,57	(XXX 1.234.567,57)
Norsk no	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	28.jan.2008 16:30:05	28. jan. 2008, 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 PST
	Date: Medium	28.jan.2008	28. jan. 2008
	Number: Negative	-1 234 567,567	-1 234 567,567
	Currency: Positive	¤ 1 234 567,57	XXX 1 234 567,57
	Currency: Negative	-¤ 1 234 567,57	XXX -1 234 567,57
	Accounting Currency: Positive	¤ 1 234 567,57	XXX 1 234 567,57
	Accounting Currency: Negative	-¤ 1 234 567,57	(XXX 1 234 567,57)
Polski pl	Date Time: Short	2008-01-28 16:30	28.01.2008, 16:30
	Date Time: Medium	2008-01-28 16:30:05	28 sty 2008, 16:30:05
	Date Time: Long	2008-01-28 16:30:05 PST	28.01.2008, 16:30:05 GMT-8
	Date: Short	2008-01-28	28.01.2008
	Date: Medium	2008-01-28	28 sty 2008
	Currency: Positive	¤ 1 234 567,57	1 234 567,57 ¤
	Currency: Negative	-¤ 1 234 567,57	-1 234 567,57 ¤
	Accounting Currency: Positive	¤ 1 234 567,57	1 234 567,57 ¤
	Accounting Currency: Negative	-¤ 1 234 567,57	(1 234 567,57 ¤)
Português pt	Date Time: Short	28-01-2008 16:30	28/01/2008 16:30
	Date Time: Medium	28/jan/2008 16:30:05	28 de jan. de 2008 16:30:05
	Date Time: Long	28-01-2008 16:30:05 PST	28/01/2008 16:30:05 GMT-8
	Date: Short	28-01-2008	28/01/2008
	Date: Medium	28/jan/2008	28 de jan. de 2008
	Date: Long	28 de Janeiro de 2008	28 de janeiro de 2008
	Currency: Positive	¤ 1.234.567,57	¤ 1.234.567,57
	Currency: Negative	-¤ 1.234.567,57	-¤ 1.234.567,57

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Accounting Currency: Positive	¤ 1.234.567,57	¤ 1.234.567,57
	Accounting Currency: Negative	-¤ 1.234.567,57	-¤ 1.234.567,57
Kiche quc	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 16:30
	Date Time: Medium	Jan 28, 2008 4:30:05 PM	Jan 28, 2008, 16:30:05
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 16:30:05 PST
	Time	4:30 PM	16:30
	Currency: Positive	¤ 1,234,567.57	\$1,234,567.57
	Currency: Negative	-¤ 1,234,567.57	-\$1,234,567.57
	Accounting Currency: Positive	¤ 1,234,567.57	\$1,234,567.57
	Accounting Currency: Negative	-¤ 1,234,567.57	(\$1,234,567.57)
Română ro	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	28.01.2008 16:30:05	28 ian. 2008, 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 GMT-8
	Date: Medium	28.01.2008	28 ian. 2008
	Currency: Positive	¤ 1.234.567,57	1.234.567,57 ¤
	Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 ¤
	Accounting Currency: Positive	¤ 1.234.567,57	1.234.567,57 ¤
	Accounting Currency: Negative	-¤ 1.234.567,57	(1.234.567,57 ¤)
Русский ru	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	28.01.2008 16:30:05	28 янв. 2008 г., 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 GMT-8
	Date: Medium	28.01.2008	28 янв. 2008 г.
	Currency: Positive	¤ 1 234 567,57	1 234 567,57 XXXX
	Currency: Negative	-¤ 1 234 567,57	-1 234 567,57 XXXX
	Accounting Currency: Positive	¤ 1 234 567,57	1 234 567,57 XXXX
	Accounting Currency: Negative	-¤ 1 234 567,57	-1 234 567,57 XXXX
Serbian (Latin) sh	Date Time: Short	1/28/2008 4:30 PM	28.1.2008. 16:30
	Date Time: Medium	jan 28, 2008 4:30:05 PM	28. 1. 2008. 16:30:05
	Date Time: Long	1/28/2008 4:30:05 PM GMT-8	28.1.2008. 16:30:05 GMT-8
	Date: Short	1/28/2008	28.1.2008.

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Date: Medium	jan 28, 2008	28. 1. 2008.
	Date: Long	januar 28, 2008	28. januar 2008.
	Time	4:30 PM	16:30
Slovenčina sk	Date Time: Short	28.1.2008 16:30	28. 1. 2008 16:30
	Date Time: Medium	28.1.2008 16:30:05	28. 1. 2008, 16:30:05
	Date Time: Long	28.1.2008 16:30:05 PST	28. 1. 2008 16:30:05 GMT-8
	Date: Short	28.1.2008	28. 1. 2008
	Date: Medium	28.1.2008	28. 1. 2008
	Date: Long	Ponedelok, 2008, januára 28	28. januára 2008
	Currency: Positive	¤ 1 234 567,57	1 234 567,57 XXX
	Currency: Negative	-¤ 1 234 567,57	-1 234 567,57 XXX
	Accounting Currency: Positive	¤ 1 234 567,57	1 234 567,57 XXX
	Accounting Currency: Negative	-¤ 1 234 567,57	(1 234 567,57 XXX)
Slovenščina sl	Date Time: Short	28.1.2008 16:30	28. 01. 2008, 16:30
	Date Time: Medium	28.1.2008 16:30:05	28. jan. 2008, 16:30:05
	Date Time: Long	28.1.2008 16:30:05 PST	28. 01. 2008, 16:30:05 GMT-8
	Date: Short	28.1.2008	28. 01. 2008
	Date: Medium	28.1.2008	28. jan. 2008
	Number: Negative	-1.234.567,567	-1.234.567,567
	Currency: Positive	¤ 1.234.567,57	1.234.567,57 ¤
	Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 ¤
	Accounting Currency: Positive	¤ 1.234.567,57	1.234.567,57 ¤
	Accounting Currency: Negative	-¤ 1.234.567,57	(1.234.567,57 ¤)
Samoan sm	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 4:30 PM
	Date Time: Medium	Jan 28, 2008 4:30:05 PM	Jan 28, 2008, 4:30:05 PM
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 4:30:05 PM PST
	Currency: Positive	¤ 1,234,567.57	\$1,234,567.57
	Currency: Negative	-¤ 1,234,567.57	-\$1,234,567.57
	Accounting Currency: Positive	¤ 1,234,567.57	\$1,234,567.57
	Accounting Currency: Negative	-¤ 1,234,567.57	(\$1,234,567.57)

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
Shqip sq	Date Time: Short	2008-01-28 4.30.MD	28.1.2008, 4:30 e pasdites
	Date Time: Medium	2008-01-28 4:30:05.MD	28 jan 2008, 4:30:05 e pasdites
	Date Time: Long	2008-01-28 4.30.05.MD PST	28.1.2008, 4:30:05 e pasdites, GMT-8
	Date: Short	2008-01-28	28.1.2008
	Date: Medium	2008-01-28	28 jan 2008
	Date: Long	2008-01-28	28 janar 2008
	Time	4.30.MD	4:30 e pasdites
	Number: Positive	1.234.567,567	1 234 567,567
	Number: Negative	-1.234.567,567	-1 234 567,567
	Currency: Positive	¤ 1.234.567,57	1 234 567,57 ¤
	Currency: Negative	-¤ 1.234.567,57	-1 234 567,57 ¤
	Accounting Currency: Positive	¤ 1.234.567,57	1 234 567,57 ¤
	Accounting Currency: Negative	-¤ 1.234.567,57	(1 234 567,57 ¤)
	Serbian (Cyrillic) sr	Date Time: Short	28.1.2008. 16.30
Date Time: Medium		28.01.2008. 16.30.05	28. 1. 2008. 16:30:05
Date Time: Long		28.1.2008. 16.30.05 PST	28.1.2008. 16:30:05 GMT-8
Date: Medium		28.01.2008.	28. 1. 2008.
Date: Long		28.01.2008.	28. јануар 2008.
Time		16.30	16:30
Currency: Positive		¤ 1.234.567,57	1.234.567,57 ¤
Currency: Negative		-¤ 1.234.567,57	-1.234.567,57 ¤
Accounting Currency: Positive		¤ 1.234.567,57	1.234.567,57 ¤
Accounting Currency: Negative		-¤ 1.234.567,57	(1.234.567,57 ¤)
Svenska sv	Date Time: Medium	2008-jan-28 16:30:05	28 jan. 2008 16:30:05
	Date Time: Long	2008-01-28 16:30:05 PST	2008-01-28 16:30:05 GMT-8
	Date: Medium	2008-jan-28	28 jan. 2008
	Date: Long	den 28 januari 2008	28 januari 2008
	Number: Negative	-1 234 567,567	-1 234 567,567
	Currency: Positive	¤ 1 234 567,57	1 234 567,57 ¤
	Currency: Negative	-¤ 1 234 567,57	-1 234 567,57 ¤

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
th	Accounting Currency: Positive	฿ 1 234 567,57	1 234 567,57 ฿
	Accounting Currency: Negative	-฿ 1 234 567,57	-1 234 567,57 ฿
	Date Time: Short	28/1/2008, 16:30 น.	28/1/2551 16:30
	Date Time: Medium	28 ม.ค. 2008, 16:30:05	28 ม.ค. 2551 16:30:05
	Date Time: Long	28/1/2008, 16 นาฬิกา 30 นาที	28/1/2551 16 นาฬิกา 30 นาที 05 วินาที GMT-8
	Date: Short	28/1/2008	28/1/2551
	Date: Medium	28 ม.ค. 2008	28 ม.ค. 2551
	Date: Long	28 มกราคม 2008	28 มกราคม 2551
	Time	16:30 น.	16:30
	Currency: Positive	฿ 1,234,567.57	XXX 1,234,567.57
	Currency: Negative	-฿ 1,234,567.57	-XXX 1,234,567.57
	Accounting Currency: Positive	฿ 1,234,567.57	XXX 1,234,567.57
Accounting Currency: Negative	-฿ 1,234,567.57	(XXX 1,234,567.57)	
Tagalog tl	Date Time: Short	1/28/2008 4:30 PM	1/28/2008, 4:30 PM
	Date Time: Medium	Jan 28, 2008 4:30:05 PM	Ene 28, 2008, 4:30:05 PM
	Date Time: Long	1/28/2008 4:30:05 PM PST	1/28/2008, 4:30:05 PM GMT-8
	Date: Medium	Jan 28, 2008	Ene 28, 2008
	Date: Long	January 28, 2008	Enero 28, 2008
	Currency: Positive	₱ 1,234,567.57	₱1,234,567.57
	Currency: Negative	-₱ 1,234,567.57	-₱1,234,567.57
	Accounting Currency: Positive	₱ 1,234,567.57	₱1,234,567.57
Accounting Currency: Negative	-₱ 1,234,567.57	(₱1,234,567.57)	
Türkçe tr	Date Time: Medium	28.Oca.2008 16:30:05	28 Oca 2008 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008 16:30:05 GMT-8
	Date: Medium	28.Oca.2008	28 Oca 2008
	Date: Long	28 Ocak 2008 Pazartesi	28 Ocak 2008
	Currency: Positive	1.234.567,57 ₺	₺1.234.567,57
	Currency: Negative	-1.234.567,57 ₺	-₺1.234.567,57
	Accounting Currency: Positive	1.234.567,57 ₺	₺1.234.567,57
	Accounting Currency: Negative	-1.234.567,57 ₺	(₺1.234.567,57)

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
Українська uk	Date Time: Short	28.01.2008 16:30	28.01.2008, 16:30
	Date Time: Medium	28 січ. 2008 16:30:05	28 січ. 2008 р., 16:30:05
	Date Time: Long	28.01.2008 16:30:05 PST	28.01.2008, 16:30:05 GMT-8
	Date: Medium	28 січ. 2008	28 січ. 2008 р.
	Date: Long	28 січня 2008	28 січня 2008 р.
	Currency: Positive	¤ 1 234 567,57	1 234 567,57 ¤
	Currency: Negative	-¤ 1 234 567,57	-1 234 567,57 ¤
	Accounting Currency: Positive	¤ 1 234 567,57	1 234 567,57 ¤
	Accounting Currency: Negative	-¤ 1 234 567,57	-1 234 567,57 ¤
Ti ng Vi t vi	Date Time: Short	16:30 28/01/2008	16:30, 28/01/2008
	Date Time: Medium	16:30:05 28-01-2008	16:30:05, 28 thg 1, 2008
	Date Time: Long	16:30:05 PST 28/01/2008	16:30:05 PST, 28/01/2008
	Date: Medium	28-01-2008	28 thg 1, 2008
	Date: Long	Ngày 28 tháng 1 năm 2008	28 tháng 1, 2008
	Currency: Positive	¤ 1.234.567,57	1.234.567,57 XXX
	Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 XXX
	Accounting Currency: Positive	¤ 1.234.567,57	1.234.567,57 XXX
	Accounting Currency: Negative	-¤ 1.234.567,57	-1.234.567,57 XXX
zh	Date Time: Short	2008-1-28 4:30	2008/1/28 16:30
	Date Time: Medium	2008-1-28 16:30:05	2008 1 28 16:30:05
	Date Time: Long	2008-1-28 04 30 05	2008/1/28 GMT-8 16:30:05
	Date: Short	2008-1-28	2008/1/28
	Date: Medium	2008-1-28	2008 1 28
	Time	4:30	16:30
	Currency: Positive	¤ 1,234,567.57	XXX 1,234,567.57
	Currency: Negative	-¤ 1,234,567.57	-XXX 1,234,567.57
	Accounting Currency: Positive	¤ 1,234,567.57	XXX 1,234,567.57

LOCALE NAME AND CODE	FORMAT TYPE	JDK FORMAT	ICU FORMAT
	Accounting Currency: Negative	-¤ 1,234,567.57	(XXX 1,234,567.57)

SEE ALSO:

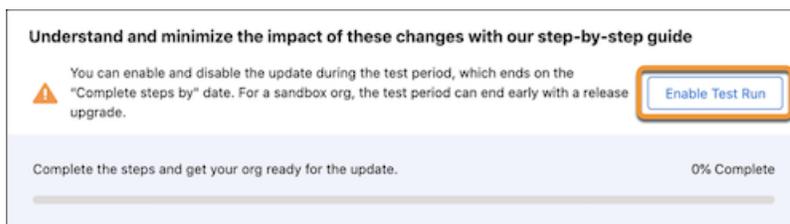
[Adopt the ICU Locale Formats](#)

Enable the ICU Locale Formats

To test the International Components for Unicode (ICU) locale formats before they're enforced in Spring '24, enable a test run in the Enable ICU Locale Formats release update. Then enable the formats for the English (Canada) locale.

When you enable the ICU locale formats, the appearance and behavior related to dates, times, and currencies can change. For this reason, we recommend that you test in a sandbox before activating the new formats in production.

1. Enable the formats for testing.
 - a. From Setup, in the Quick Find Box, enter *Release Updates*, and then select **Release Updates**.
 - b. For the Enable ICU Locale Formats release update, click **Get Started**.
 -  **Note:** If the Enable ICU Locale Formats release update only appears on the Archived tab, the formats are enabled.
 - c. In the "Understand and minimize the impact of these changes with our step-by-step guide" section, click **Enable Test Run**.



After you click **Enable Test Run**, the same section includes the text, "This update is now enabled for testing." Your org is using ICU formats.

2. Activate the ICU formats for the English (Canada) [en_CA] locale.
 - a. In the Quick Find box, enter *User Interface*, and then select **User Interface**.
 - b. Select **Enable ICU formats for en_CA locale**, and save your changes.

SEE ALSO:

[Adopt the ICU Locale Formats](#)

[ICU Locale Format Migration Tests](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

USER PERMISSIONS

To view release updates:

- View Setup and Configuration

To enable or disable release updates

- Manage Release Updates

OR

Customize Application

API Versions for Apex Classes, Apex Triggers, and Visualforce Pages

The International Components for Unicode (ICU) locale formats are available with API version 45.0 and later. To use the ICU locale formats in your customizations, update your Apex classes, Apex triggers, and Visualforce pages to the latest API version. If these components use API version 44.0 or earlier, they return Oracle's Java Development Kit (JDK) locale formats, which can cause data integrity issues and end-user confusion.

Apex, Visualforce Pages, and API Versions

Apex is a programming language that enables developers to add business logic to most system events, including button clicks, related record updates, and Visualforce pages. Apex code can be initiated by Web service requests and from triggers on objects.

- An Apex class is a template or blueprint from which Apex objects are created. Classes consist of other classes, user-defined methods, variables, exception types, and static initialization code.
- An Apex trigger is code that executes before or after specific data manipulation language (DML) events occur. For example, before object records are inserted into the database or after records have been deleted. Triggers are stored as metadata in Salesforce.

A Visualforce page is similar to a standard Web page, but it includes powerful features to access, display, and update your organization's data. You can use Visualforce pages to customize your org's front-end UI and functionality. Lightning Web Components (LWC) is the preferred way to build UI with Salesforce. If you have Visualforce pages, confirm that each page is in use before you analyze and update it. To learn more about LWC and complying with current web standards, go to the [Migrate from Visualforce to Lightning Web Components](#) trail.

Independent software vendors (ISV) also use Apex classes, Apex triggers, and Visualforce pages to deliver functionality within their packages. ISVs are responsible for updating the API versions of their package components.

Each Visualforce page, Apex class, and Apex trigger has an API version. The initial API version is always the API version of your Salesforce org when the component is created.

A new API version is available with each Salesforce release. However, Salesforce doesn't update the API version of your Apex classes, Apex triggers, and Visualforce pages because we can't test them for any potential issues. Ideally, you update the API version for your components and validate the code with each release, but sometimes that doesn't happen. Therefore, for example, it's possible for an Apex class to use API version 21.0 in an org on API version 53.0.

Potential Errors

If you don't upgrade your Apex classes, Apex triggers, and custom Visualforce pages to API version 45.0 or higher, your users can receive a ParseException error. For example, "Invalid Date and Time." These errors don't cause data integrity issues, but the errors can frustrate users.

Custom date/time fields edited in Salesforce Classic and inline edits on Visualforce pages always use the latest API version. Because of that behavior, when ICU is enabled, these custom fields and inline edits always use the ICU locale formats, regardless of the page's API version. Your users can experience a ParseException error in two situations:

- The user makes an inline edit on a Visualforce page on API version 44.0 or earlier and saves their changes.
- The user enters a date/time in a custom field in Salesforce Classic.

To avoid these issues when ICU is enabled, ensure that your Apex classes, Apex triggers, and custom Visualforce pages use API version 45.0 or later.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

USER PERMISSIONS

To define, edit, delete, set security, and set version settings for Apex classes:

- Author Apex

To run Apex tests:

- View Setup and Configuration

To view Apex triggers:

- View Setup and Configuration

To edit Apex triggers:

- Author Apex

ICU API Version Requirement

Salesforce added the ICU locale formats in Spring '19, which corresponded to API version 45.0. When the ICU locale formats are enabled, all Salesforce delivered functionality uses the ICU formats. However, Apex classes, Apex triggers, and Visualforce pages only use the ICU locale formats when ICU is enabled and the API version is 45.0 or later.

Custom code and components that use API version 44.0 or earlier can't reference the ICU locale formats because they don't exist in that API version. In that case, the custom code and components return the JDK locale formats.

Let's look at an example.

The JDK and ICU short date formats for the Spanish (United States) [es_US] locale differ. The numbers representing the month and day are swapped.

- JDK short date format for es_US: MM/dd/yyyy (example: 1/28/2008)
- ICU short date format for es_US: dd/MM/yyyy (example: 28/1/2008)

In this example, an Opportunity has a close date of November 2, 2021. This simple custom Visualforce page includes the Close date field on the Opportunity object. The displayed information differs based on the API version of the Visualforce page.

Here's API version 45 or later.

Custom Opportunity Info page	
▼ Opportunity Info	
Opportunity Name	Office equipment order
Close Date	2/11/2021
Stage	Closed Won
Amount	\$400,000.00

The Visualforce page uses the ICU locale short date format: dd/MM/yyyy, or 2/11/2021.

And here's the same screen with API version 44 or earlier.

Custom Opportunity Info page	
▼ Opportunity Info	
Opportunity Name	Office equipment order
Close Date	11/2/2021
Stage	Closed Won
Amount	\$400,000.00

Because the ICU locale formats aren't available in API version 44, the system shows the JDK short date format: MM/dd/yyyy, or 11/2/2021.

In this example, the user expects the day of the month to be listed first. If the Visualforce page uses API version 44.0 or earlier, the user can misinterpret the date as February 11, 2021 instead of November 2, 2021. Inline edits on Visualforce pages always use the latest API version. Because of that behavior, when ICU is enabled, inline edits on Visualforce pages always use the ICU locale formats, regardless of the page's API version. When a user makes an inline edit on a Visualforce page on API version 44.0 or earlier and saves their changes, the user can receive a ParseException error. For example, "Invalid Date and Time." These errors don't cause data integrity issues, but the errors can frustrate users. To avoid this issue when ICU is enabled, ensure that your custom Visualforce pages use API version 45.0 or later.

Sources

There are two sources for Apex classes, Apex triggers, and Visualforce pages in your org. Either someone built them directly in your org, or they were included in a managed package that was installed.

Only package owners can edit the components included in a managed package. You can see items installed by a managed package in your lists, but you can't edit them. To get updates to those items, you must install a new version of the package that contains the updates.

If you're a package owner, update your package to use the latest API version in Apex classes, Apex triggers, and Visualforce pages that reference dates, times, integers, and currencies.

[Check for API Versions](#)

Not sure whether your org has Apex classes, Apex triggers, and Visualforce pages? Each has a list in Setup that includes the version number.

[Update the API Version](#)

API version 45.0 is the minimum required version for ICU.

SEE ALSO:

[Adopt the ICU Locale Formats](#)

[Visualforce Developer Guide](#)

Check for API Versions

Not sure whether your org has Apex classes, Apex triggers, and Visualforce pages? Each has a list in Setup that includes the version number.

- To see your Apex classes, from Setup, in the Quick Find box, enter *Apex Classes*, and then select **Apex Classes**.
- To see your Apex triggers, from Setup, in the Quick Find box, enter *Apex Triggers*, and then select **Apex Triggers**.
- To see your Visualforce pages, from Setup, in the Quick Find box, enter *Visualforce Pages*, and then select **Visualforce Pages**.

The version number is shown in the Version field. If a list is empty, you don't have any of those items.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

USER PERMISSIONS

To define, edit, delete, set security, and set version settings for Apex classes:

- Author Apex

To run Apex tests:

- View Setup and Configuration

To view Apex triggers:

- View Setup and Configuration

To edit Apex triggers:

- Author Apex

Apex Triggers Help for this Page

This page allows you to view and modify all the triggers in your organization. To create a new trigger, navigate to the appropriate sObject triggers page.

✔ **Percent of Apex Used: 0.01%**
 You are currently using 523 characters of Apex Code (excluding comments and @isTest annotated classes) in your organization, out of an allowed limit of 6,000,000 characters. Note that the amount in use includes both Apex Classes and Triggers defined in your organization.

Compile all Triggers (1) View: All | Create New View

Action	Name	Namespace Prefix	sObject Type	Api Version	Status	Size Without Comments	Last Modified By	Has Trace Flags
Edit Del	SetDealPrediction		Opportunity	44.0	Active	61	Chloe McKinney, 10/23/2021, 1:38 PM	<input type="checkbox"/>
	ADM_TaskDeletingTrigger	agf	ADM_Task	23.0	Active	677	Chloe McKinney, 10/8/2020, 12:57 PM	<input type="checkbox"/>
	ADM_TaskTrigger	agf	ADM_Task	19.0	Active	6,462	Chloe McKinney, 10/8/2020, 12:57 PM	<input type="checkbox"/>
	ADM_TeamDependency	agf	ADM_Team_Dependency	16.0	Active	9,681	Chloe McKinney, 10/8/2020, 12:57 PM	<input type="checkbox"/>
	ADM_ThemeAssignmentCRUDCheck	agf	ADM_Theme_Assignment	28.0	Inactive	469	Chloe McKinney, 10/8/2020, 12:57 PM	<input type="checkbox"/>
	ADM_ThemeAssignmentTrigger	agf	ADM_Theme_Assignment	26.0	Active	3,090	Chloe McKinney, 10/8/2020, 12:57 PM	<input type="checkbox"/>
	ADM_ThemeCRUDCheck	agf	ADM_Theme	28.0	Inactive	426	Chloe McKinney, 10/8/2020, 12:57 PM	<input type="checkbox"/>
	ADM_ThemeTrigger	agf	ADM_Theme	26.0	Active	3,556	Chloe McKinney, 10/8/2020, 12:57 PM	<input type="checkbox"/>
	ADM_UserTrigger	agf	User	28.0	Inactive	67	Chloe McKinney, 10/8/2020, 12:57 PM	<input type="checkbox"/>
	ADM_WorkCRUDCheck	agf	ADM_Work	28.0	Inactive	427	Chloe McKinney, 10/8/2020, 12:57 PM	<input type="checkbox"/>

In this example, a user created the first Apex trigger in the list, SetDealPrediction, and the other triggers were included in a managed package. How can we tell? The other triggers have a Namespace Prefix, which indicates that they're part of an installed package.

To quickly identify the items on API version 44.0 or earlier that you can modify, create a view. This example shows creating a filter for the Apex Triggers list. You can use the same process for the Apex Classes list and the Visualforce Pages list.

1. Click **Create New View**.
2. In View Name, enter a view name. For example, *Non-packaged, API v44 or earlier*.
3. In View Unique Name, enter a unique name to identify this view for the API. For example, *apex_triggers_nopackage_api44_or_earlier*.
4. On the first line, for Field, select **Api Version**. For Operator, select **less or equal**. And for Value, enter *44.0*. On the second line, for Field, select **Installed Package**. For Operator, select **equals**, and leave Value blank.

Step 2. Specify Filter Criteria Field Filters Help ?

Filter By Additional Fields (Optional):

Field	Operator	Value	
Api Version	less or equal	44.0	AND
Installed Package	equals		AND
--None--	--None--		AND
--None--	--None--		AND
--None--	--None--		

[Add Filter Logic...](#)

If you're a partner or developer who owns a managed package, for Value, enter your Installed Package name. Or you can filter on your Namespace Prefix.

5. Optionally, select the fields to display in the list.
6. In **Step 4. Restrict Visibility**, specify whether you want this view to be visible to only you, to all users, or to certain groups of users.
7. Save your changes.

The list now shows items with an API version of 44.0 or earlier that aren't part of an installed package. Or, if you specified an Installed Package in your filter, the list shows only items included in that package.

Update the API Version

API version 45.0 is the minimum required version for ICU.

We recommend that you adopt the latest API version available, if possible. If your current API version is much earlier than the new API version, incremental upgrades can help you identify the relevant changes to test.

You can update the API version of Apex classes, Apex triggers, and Visualforce pages from the corresponding Setup page. Updating the API version can include structural and behavior changes for objects and other code components. For example, an API change can add or remove fields on an object, introduce new outputs, or change the behavior of a field. We recommend that you back up your code before you upgrade the API version. Perform the upgrade in a sandbox, and complete thorough testing of all related functionality before you update production.

To determine whether an item uses locales, look for fields and code returning these types of data. The JDK and ICU locale formats for these types differ.

- Date
- Time
- Datetime
- Number (Integer)
- Currency
- Accounting Currency
- Next to the component's name, click **Edit**, then select the **Version Settings** tab.

If you have Visualforce pages, confirm that they're being used before you analyze and update them. Next to the page name, click **Edit**, then click **Where is this used?**

1. Go to the Apex Classes, Apex Triggers, or Visualforce Pages Setup page.
2. Next to the component's name, click **Edit**, then select the **Version Settings** tab.
3. In the Version field for Salesforce.com API, select version 45.0 or later.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

USER PERMISSIONS

To define, edit, delete, set security, and set version settings for Apex classes:

- Author Apex

To run Apex tests:

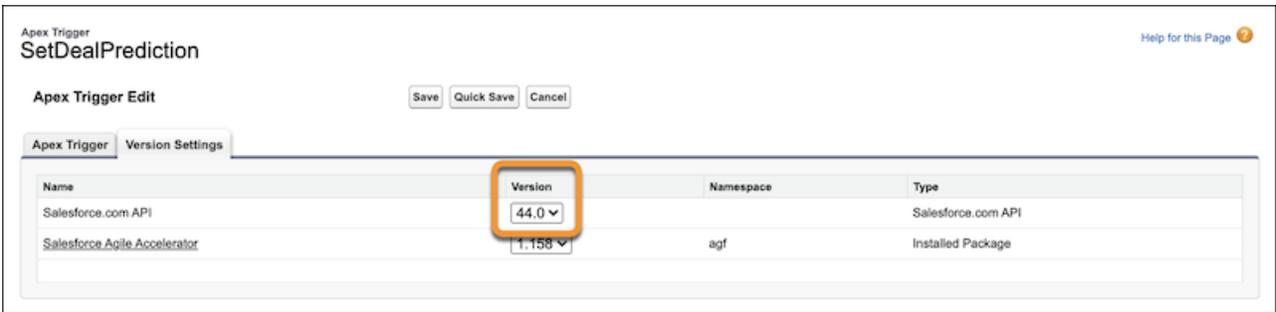
- View Setup and Configuration

To view Apex triggers:

- View Setup and Configuration

To edit Apex triggers:

- Author Apex



4. Save your changes.

Test the class, trigger, or page, and verify that all related functionality works with the new API version.

Custom Code and Locale Format Changes

Address, currency, date, datetime, integer, name, and time formats can change when a user changes locales. These formats can also change when the locale format standard changes or formats are updated. Learn how to avoid errors by using locale-neutral methods in your code and review examples. Then understand how to verify that your integrations work with new or changed formats.

[Use Locale-Neutral Methods in Code](#)

Data formats can change based on the user's locale, adoption of new standards, or updates to the standard locale formats. To avoid errors when a locale format changes, use standard methods to handle this data in your code. If your code formats the data using the user's locale, apply the format after all other processing is complete.

[Example Code with Locale-Formatted Data](#)

Review examples of code that handles data that can be formatted based on the user's locale. See how code can break when it relies on a specific format for dates, times, and currencies. And review examples of how to fix these issues by using standard methods for handling these types of data.

[Update Your Integrations for New Locale Formats](#)

If you integrate data from external systems into Salesforce or if you send Salesforce data to external third parties, use locale-neutral formats whenever possible in the related code. When locale formats change, review the code that handles the affected formats.

SEE ALSO:

[Adopt the ICU Locale Formats](#)

[API Versions for Apex Classes, Apex Triggers, and Visualforce Pages](#)

Use Locale-Neutral Methods in Code

Data formats can change based on the user's locale, adoption of new standards, or updates to the standard locale formats. To avoid errors when a locale format changes, use standard methods to handle this data in your code. If your code formats the data using the user's locale, apply the format after all other processing is complete.

To search your Salesforce code, download the metadata. Then use a command-line interface such as [Salesforce CLI](#).

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

A user's locale determines the formats for these types of data: address, currency, date, datetime, name, integer, and time. The start day of the week is also based on the user's locale.

When you migrate from Oracle's Java Development Kit (JDK) locale formats to the International Components for Unicode (ICU) locale formats, the currency, date, datetime, integer, and time formats change for some locales.

Also, locale formats are regularly updated to match the newest international standards. And users can update their locale to match their current location or preference.

To prevent issues with your custom code due to locale format changes, follow these guidelines.

- Use standard methods to call these formats. For example, when handling dates in Apex, use the `Date` data type.
- When handling these data types in your code, use standard methods to extract components. For example, when you want to extract the month from a date format in Apex, use the `month()` method on the `Date` class. Similarly, handle integers and currency values as unformatted integers until you must format them.
- If your code performs additional processing on a value, use a locale-neutral format. For example, in Apex, use `format(string dateFormat)` or `format(string dateFormat, string timezone)`.
- Make the transformation of data to the user's preferred locale format the last step in handling that data. For example, when calculating a future date in Apex, use the `format()` method of the `Date` class after the calculation.
- Apex `format()` methods, such as `DateTime.format()` return values in the context user's locale. If subsequent code expects data in a particular locale format, specify the format explicitly. For example, to pass a time in a format such as `10:15 a` in Apex, use `DateTime.format('h:mm a')`. Because this example passes the string argument `'h:mm a'` to the format function, the datetime is formatted according to the supplied format regardless of the context user's locale.
- When constructing delimited lists, put any locale data that can contain a comma in quotes.

Here are some examples of code that return formats in the user's preferred locale format.

- Apex: the `format()` method in the `Date`, `DateTime`, and `Integer` classes
- Aura Lightning Components: the `$Locale` global variable
- Lightning Web Component Internationalization properties

SEE ALSO:

[Example Code with Locale-Formatted Data](#)

[Update Your Integrations for New Locale Formats](#)

[Apex Reference Guide](#)

[Lightning Aura Components Developer Guide: \\$Locale](#)

[Salesforce Lightning Component Library: Access Internationalization Properties](#)

Example Code with Locale-Formatted Data

Review examples of code that handles data that can be formatted based on the user's locale. See how code can break when it relies on a specific format for dates, times, and currencies. And review examples of how to fix these issues by using standard methods for handling these types of data.

Currency, date, time, datetime, integer, name, and address formats can change when a user changes locales. When you enable the International Components for Unicode (ICU) locale formats, the date, time, datetime, integer, and currency formats change for some locales.

Let's look at some code examples that handle these data types and the errors that can occur if we don't [use locale-neutral methods in code](#).

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

Extract Components of a Date

In this example, we want to validate a date: October 12, 2021. To keep the example simple, we show only a portion of the process, where the code validates the month, day, and year values. The month value must be less than or equal to 12. The day value must be less than or equal to 31. And the year value must have exactly 4 digits. Only dates that pass all three tests are then extracted to the respective values for additional processing.

Here's an example that uses the Apex Pattern and Matching classes to determine the date. The pattern matching assumes that the date format is MM/dd/yyyy.

```
Date myDate = Date.newInstance(2021, 10, 20);
String formattedDate = myDate.format();

//Simple regex not having all validations for days in months nor accounting for leap year
Pattern datePattern =
Pattern.compile('(0?[1-9]|1[0-2])\\/(0?[1-9]|[2][0-9]|3[01])\\/([0-9]{4})');
Matcher matcher = datePattern.matcher(formattedDate);

if(matcher.matches()) {
    Integer day = Integer.valueOf(matcher.group(1)); //10
    Integer month = Integer.valueOf(matcher.group(2)); //20
    Integer year = Integer.valueOf(matcher.group(3)); //2021
    // Further validation logic for max days in month/ leap year and post processing
}
```

Apex code formats the date according to the context user's locale. In this example, the context user has chosen the Spanish (United States) [es_US] locale.

When the ICU locale formats are enabled, this validation fails. The ICU format for the user's locale is different than the corresponding Oracle's Java Development Kit (JDK) format.

- JDK short date format for es_US: 10/20/2021
- ICU short date format for es_US: 20/10/2021

The `format()` method of the Apex Date class returns the date as a string using the locale of the context user. In this case, because the ICU locale formats are enabled and the user's locale is es_US, it returns 20/10/2021.

The code then uses the placement in the date output to assign the month, day, and year values, assuming a format of MM/dd/yyyy. So the code assigns 20 as the month, and because 20 is greater than 12, the pattern matching incorrectly determines that this date is invalid.

To avoid these kinds of issues, use the built-in Apex methods to extract the required values. In this case, `month()`, `day()`, and `year()`.

Here's an example of using those methods to set the month, day, and year values.

```
Date myDate = Date.newInstance(2021, 10, 20);

// assign month, day, and year values for validation
Integer month = myDate.month(); //10
Integer day = myDate.day(); //20
Integer year = myDate.year(); //2021

// Further validation logic
```

Validate a Datetime Value

This Apex example uses the `Datetime.parse` method to create a datetime from a string. The passed value matches the JDK locale format for the English (United States) [en_US] locale.

This validation fails when the ICU locale formats are enabled, because the datetime format for en_US is different between JDK and ICU. The ICU format includes a comma after the date.

- JDK datetime format for es_US: 10/14/2011 11:46 AM
- ICU datetime format for es_US: 10/14/2011, 11:46 AM

```
Datetime dt = DateTime.parse('10/14/2011 11:46 AM');
String myDtString = dt.format();
system.assertEquals(myDtString, '10/14/2011, 11:46 AM');
```

To fix this issue, update the passed value to the ICU locale format. If an external system is passing the value, contact the sender to update the format of the source data. Whenever possible, ask the sender to send the date in a locale-neutral format. It's best to handle format updates this way because locale-neutral formats don't require updates to your code when the format changes.

However, it's not always possible to have the sender update the format of the data passed to your org. If that happens, because you know the format of the data being sent, you can reformat it. In these cases, convert the data into a locale-neutral format.

Here are two common methods used to format a datetime in Apex. With both of these methods, the resulting datetime is locale-neutral: it's displayed in the user's chosen locale. For more information about the methods available for all formats, see the Apex Reference Guide.

- Extract the date components to separate parameters: year, month, day, hours, minutes, and seconds. Then, to create a locale-neutral date, use the `DateTime.newInstanceGMT()` method of the `Datetime` Apex class.

```
//Before using the code below, set the year, month, day, hour, minutes, and seconds
components
//by extracting values from the passed date and complete any necessary validation

//set the datetime value by passing the parameters
DateTime myDt = DateTime.newInstanceGMT(year, month, day, hour, minutes, seconds);
```

- Reformat the passed data in the standard date format `yyyy-MM-dd HH:mm:ss` in the locale time zone. Then, to create a locale-neutral date, use the `valueOf(String dateTimeString)` method of the `Datetime` class.

```
//Before using the code below, convert the passed datetime data to a string in the format
yyyy-MM-dd HH:mm:ss
//and assign that value to the stringDate parameter

//set the datetime value by passing the string
DateTime myDt = date.valueOf(stringDate);
```

This approach to converting formats works as long as the format of the data passed to your org doesn't change. If your external source updates their format, you must update the methods you use to extract or convert the data.

Pass a Time to an External System

In this simple example, an event is occurring at 3:30 PM GMT on November 18, 2021. We want to pass the date and time as separate values to an external system.

```
//create Datetime to pass externally in GMT
DateTime event1_dt = DateTime.newInstanceGMT(2021, 11, 18, 15, 30, 0);

//split into event date and event time for external system
```

```
Date event1_date = event1_dt.date();
Time event1_time = event1_dt.time();
```

This code works if the external system expects the date and time in neutral formats. But what if the external system needs the date and time of an event in a specific format? Let's assume that the external system expects the date and time in these formats: 18/11/2021 and 3:30 PM.

In this case, to apply the expected formats to the event date and time, use the `Datetime format ()` method.

```
//create Datetime to pass externally
DateTime event1_dt = DateTime.newInstance(2021, 11, 18, 15, 30, 0);

//split into event date and event time for external system, applying expected format
String event1_date = event1_dt.format('dd/MM/yyyy');
String event1_time = event1_dt.format('h:mm a');
```

SEE ALSO:

[Use Locale-Neutral Methods in Code](#)

[Update Your Integrations for New Locale Formats](#)

[Apex Reference Guide](#)

Update Your Integrations for New Locale Formats

If you integrate data from external systems into Salesforce or if you send Salesforce data to external third parties, use locale-neutral formats whenever possible in the related code. When locale formats change, review the code that handles the affected formats.

Integration points can take many forms, including API calls to and from Salesforce. Also review processes that include exporting data into files, such as comma-separated values (CSV) files, and importing data from files into Salesforce.

Address, currency, date, datetime, integer, Name, and time formats can change when a user changes locales. Whenever possible, use standard locale-neutral methods to handle these types of data. In the absence of a standard method, update the code to accommodate the new formats.

Specific to migrating from Oracle's Java Development Kit (JDK) formats to International Components for Unicode (ICU) locale formats, verify integrations that handle currency, date, datetime, integer, or time data.

If a third party calls into Salesforce programmatically, work with that party to test and update the process as needed when locale formats change. To search your Salesforce code, download the metadata. Then use a command-line interface such as [Salesforce CLI](#).

Integration Example: Importing Dates

Let's look at a simple example of how a change in a locale format can affect integrations.

In this example, we have a custom object, Conference, with two additional fields: `start_date_time` and `end_date_time`. To populate the Conference object, an Apex class fetches data using an external API. The class could also fetch the data from a CSV file, but in this example, we use an external API call.

The external API call returns a JSON object that contains this information. The datetime data is formatted using the JDK format for the English (United States) [en_US] locale.

```
{
  "conferences": [{
    "name": "conference1",
```

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

```

        "start_date_time": "10/20/2021 10:00 AM",
        "end_date_time": "10/22/2021 05:00 PM"
    }, {
        "name": "conference2",
        "start_date_time": "11/21/2021 11:00 AM",
        "end_date_time": "11/24/2021 05:00 PM"
    }
}

```

This Apex code inserts the conference records.

```

// Mocking the sample response of API call
String jsonResponse = '{"conferences": [{"name":"conference1", "start_date_time":"10/20/2021
10:00 AM", "end_date_time":"10/22/2021 5:00 PM"}, {"name":"conference2",
"start_date_time":"11/21/2021 11:00 AM", "end_date_time":"11/24/2021 05:00 PM"}]}'

Map<String, Object> results = (Map<String, Object>) JSON.deserializeUntyped(jsonResponse);

List<Object> conferences = (List<Object>) results.get('conferences');

for(Object conference: conferences) {
    Map<String, Object> conferenceDetails = (Map<String, Object>)conference;

    //Initialize object
    Conference__c confObject = new Conference__c (
        name = String.valueOf(conferenceDetails.get('name')),
        start_date_time__c =
datetime.parse(String.valueOf(conferenceDetails.get('start_date_time'))),
        end_date_time__c = datetime.parse(String.valueOf(conferenceDetails.get('end_date_time')))
    );

    //insert object
    insert confObject;
}

```

The `datetime.parse()` method uses the datetime format of the personal locale of the user that executes the code.

Let's assume that the user's personal locale is English (United States) [en_US]. The JDK and ICU datetime formats for that locale differ.

- JDK short datetime format for en_US: 10/20/2021 10:00 AM
- ICU short datetime format for en_US: 10/20/2021, 10:00 AM

When the org uses JDK locale formats, this code runs successfully. When ICU locale formats are enabled, this code throws a parse error because the `start_date_time` and `end_date_time` values are missing the expected comma after the year.

This issue can also occur when data stored in Salesforce is passed to an external system using a locale-specific format, for example, when using a POST call. As with the example above, the personal locale of the user that executes the code determines the format of the data.

Remediate Issues

To avoid these issues, use locale-neutral formats when receiving, passing, and processing data.

If you find an issue with data received from an external system, contact the sender to update the format of the source data. If you can't contact the sender, update your code to convert the received data into a locale-neutral format before processing it.

SEE ALSO:

- [Use Locale-Neutral Methods in Code](#)
- [Example Code with Locale-Formatted Data](#)
- [Salesforce Developer Center: Apex](#)
- [Adopt the ICU Locale Formats](#)

ICU Locale Format Migration Tests

To avoid unexpected behavior after you migrate from Oracle's Java Development Kit (JDK) locale formats to International Components for Unicode (ICU) locale formats, test the ICU locales. When you migrate from JDK to ICU, the formats for some locales change. Use functional tests to verify existing functionality, and confirm that these formats appear correctly for each affected locale used in your org. Also, verify that integration with third parties works as expected, and test your installed packages with the new formats.

Test in a Sandbox

Because dates, times, numbers, and currencies are used throughout Salesforce, it's important that you test thoroughly in a sandbox when you enable the ICU locale formats. Run the same tests for each locale used in your org.

Also consider asking users for each locale used in your org to verify that the formats appear as expected. Identify key workflows, reports, filters, and screens, and help the users understand the fields and functionality that uses the affected data types.

Verify That Your Installed Packages Are Ready for ICU

If you have installed packages from AppExchange, check with your package providers. Before you start testing, make sure that all your installed packages are compatible with the ICU locale formats. If your package provider indicates that a fix related to ICU is pending for one of your installed packages, factor that information into your testing and activation timeline.

Look for These Issues

When you enable the ICU locale formats, the formats for these data types change for some locales: currency, date, datetime, integer (numbers), and time. If you're testing for a locale format change, the address and name data types can also change.

Although the specifics can vary, issues usually fall into one of these buckets.

- Unexpected formats. In the section on functional and end-user testing, we call out specific areas to test. Most unexpected formats occur on custom pages, during custom triggered events, or are returned by custom objects when a Visualforce page, Apex class, or Apex trigger uses API version 44.0 or earlier. For more information and examples, see [API Versions for Apex Classes, Apex Triggers, and Visualforce Pages](#).
- Custom code exceptions and errors. Good code practices use locale-neutral methods when handling data and apply locale-specific formats after all other processing is complete. For this reason, issues with custom code aren't common. However, some custom code can handle locale data improperly. To learn how to use locale-neutral methods in your code and review examples, see [Custom Code and Locale Format Changes](#).

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

USER PERMISSIONS

To view release updates:

- [View Setup and Configuration](#)

To enable or disable release updates

- [Manage Release Updates](#)

OR

[Customize Application](#)

Consider End Users and Processes

When testing, consider how the new locale formats can impact your end users and processes. For example, an uninformed user can misinterpret a new date format, or a longer format can require adjustments to printed labels. When possible, we recommend that you include end users in your testing. End users can help test their workflows and help identify the potential impact of the new locale formats on your processes.

To help your end users prepare and reduce post-activation questions, notify your users before you enable the new formats in production. Provide detailed information about the changes to the locales in use in your org, and point them to any updated processes.

To determine the locales in use in your org and which users the new locale formats impact, see [Determine the Locales in Use](#).

Functional and End-User Testing

In addition to your standard functional testing, make sure to include custom functionality that relies on currency, date, datetime, integer (numbers), and time data. For example, a workflow that runs based on the day of the month or a report that groups Opportunities by value.

Ensure that your test plan includes these areas that locale format changes can impact.

- **Filters**—Filters are available in reports, formulas, validation checks, and automated workflows. Also, filters can exist in lookup relationship fields. Test filters that use dates, times, numbers, and currency values.
- **Apex Code and Lightning Components**—When testing, include all custom functionality written by a developer using Apex or Lightning components. Custom code can include Lightning components and pages, Visualforce pages, custom workflows, and reports.
- **Processes That Use Third-Party Data**—Receiving data from an external system is another type of integration. Identify and test processes that use incoming data from an external party. For example, if you receive leads from an external vendor. This data can be integrated into Salesforce automatically through API calls, or it can come in the form of files to be processed, such as CSV files.
- **Third-Party Apps That Use Salesforce Data**—Check your existing integrations to ensure that your data is correctly parsed with the new formats. Most integrations store data in a neutral format, but some integrations specify the format of the data for input and output.

For example, you send information about your contacts to a third party that then sends reminders based on contract dates. During your testing, verify that the third-party app receives the data with the modified locale date formats correctly. If you find an issue with a third-party app, contact the company that owns the app to remediate the issue.

- **Installed Packages**—If your org has installed packages from AppExchange, verify that your data is parsed correctly with the new formats.

For example, if an installed package provides or scrubs lead data, verify that the date, time, and currency data display as expected with the new formats. Or, if the package provides project management tools, test any date-based calculations. If you encounter an issue with a managed package, report the issue to the package provider.

- **Custom Functionality**—Validate web services, email services, formula-based fields, and any complex business workflows in Salesforce that use custom code. Focus on the processing of date, time, number, and currency data, and include processes that are triggered based on this data.

Test Again in Production

Before you enable ICU in production, we highly recommend that you test the ICU locale formats in a sandbox. Ideally, your sandbox includes all the functionality of production, but there can be obvious and not so obvious differences with production. For example, does your sandbox include integration with all third-party applications? Are there data types or complexities that only exist in production? As a result, we recommend that you perform another round of testing when enabling the ICU locale formats in production.

Complete the Release Update

After you enable the ICU locale formats, complete your testing, and update your org as needed, you can complete the Enable ICU Locale Formats release update. In Setup, in the Quick Find box, enter *Release Updates*, and then click **Release Updates**. For Enable ICU Locale Formats, click **Get Started**. Click the **Assess the impact of this release update** step, and click **Done**. Then confirm that you completed the required steps for the update. After you complete the update, the steps can't be changed.

SEE ALSO:

[Adopt the ICU Locale Formats](#)

[Custom Code and Locale Format Changes](#)

Salesforce Supported Locales and ICU Formats

Salesforce supported locales and their corresponding International Components for Unicode (ICU) formats for name, address, numbers, currencies, dates, and times. We use ICU version 71.1, which uses the Unicode Common Locale Data Repository (CLDR) version 41. These formats are available upon activation of the Enable ICU Formats critical update and require version 45.0 or later of the Salesforce platform API.

[Supported Number, Name, and Address Formats \(ICU\)](#)

Salesforce supported locales with their International Components for Unicode (ICU) formats for numbers, name, and address.

[Supported Date and Time Formats \(ICU\)](#)

The start day of the week and the International Components for Unicode (ICU) date and time formats for each Salesforce supported locale.

Supported Number, Name, and Address Formats (ICU)

Salesforce supported locales with their International Components for Unicode (ICU) formats for numbers, name, and address.

 **Note:** Review these important details about the data in this table.

- We recommend viewing this information in Salesforce Help. Not all characters appear correctly in PDFs.
- Arabic-Indic is the numeral system for certain locales and languages. If you want to use the Hindu-Arabic numeral system for those languages and locales, contact Salesforce Customer Support.

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
Afrikaans (Suid-Afrika) af_ZA	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country

EDITIONS

Available in: Lightning Experience and Salesforce Classic ([not available in all orgs](#))

Available in: **Group, Professional, Enterprise, Performance, Unlimited, Database.com,** and **Developer** Editions

EDITIONS

Available in: Lightning Experience and Salesforce Classic ([not available in all orgs](#))

Available in: **Group, Professional, Enterprise, Performance, Unlimited, Database.com,** and **Developer** Editions

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
() am_ET	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
)) ar_AE	-	Ms. FName LName	Address Line 1, Address Line 2 State ZipCode City Country
)) ar_BH	-	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
)) ar_DZ	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
)) ar_EG	-	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
)) ar_IQ	-	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
)) ar_JO	-	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
)) ar_KW	-	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
)) ar_LB	-	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
)) ar_LY	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
)) ar_MA	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
)) ar_OM	-	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
)) ar_QA	-	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
)) ar_SA	-	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
)) ar_SD	-	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			Country
)) ar_SY	-	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
)) ar_TN	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
)) ar_YE	-	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Azerbaijani (Azerbaijan) az_AZ	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Belarusian (Belarus) be_BY	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Български (България) bg_BG	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
() bn_BD	, , , . - , , , .	Ms. FName LName	Address Line 1, Address Line 2 City - ZipCode State Country
() bn_IN	, , , . - , , , .	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			State Country
Bosanski (Bosna i Hercegovina) bs_BA	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Català (Espanya) ca_ES	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Čeština (Česko) cs_CZ	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Cymraeg (Y Deyrnas Unedig) cy_GB	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
Dansk (Danmark) da_DK	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Deutsch (Österreich) de_AT	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Deutsch (Belgien) de_BE	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
Deutsch (Schweiz) de_CH	1'234'567.567 -1'234'567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Deutsch (Deutschland) de_DE	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Deutsch (Luxemburg) de_LU	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Dzongkha (Bhutan) dz_BT	, , . - , , .	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Ελληνικά (Κύπρος) el_CY	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Ελληνικά (Ελλάδα) el_GR	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
English (United Arab Emirates) en_AE	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 State ZipCode City Country
English (Antigua & Barbuda) en_AG	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
English (Australia) en_AU	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
English (Barbados) en_BB	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Belgium) en_BE	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Bermuda) en_BM	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Bahamas) en_BS	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Botswana) en_BW	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Belize) en_BZ	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Canada) en_CA	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
English (Cameroon) en_CM	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Cyprus) en_CY	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
English (Germany) en_DE	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
English (Eritrea) en_ER	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Fiji) en_FJ	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Falkland Islands) en_FK	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (United Kingdom) en_GB	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
English (Ghana) en_GH	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Gibraltar) en_GI	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Gambia) en_GM	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Guyana) en_GY	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Hong Kong SAR China) en_HK	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Indonesia) en_ID	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
English (Ireland) en_IE	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
English (Israel) en_IL	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			ZipCode City State Country
English (India) en_IN	12,34,567.567 -12,34,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Italy) en_IT	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
English (Jamaica) en_JM	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
English (Kenya) en_KE	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Cayman Islands) en_KY	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 State ZipCode City Country
English (Liberia) en_LR	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
English (Madagascar) en_MG	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			State Country
English (Malta) en_MT	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Mauritius) en_MU	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
English (Malawi) en_MW	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Malaysia) en_MY	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
English (Namibia) en_NA	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Nigeria) en_NG	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Netherlands) en_NL	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
English (New Zealand) en_NZ	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Papua New Guinea) en_PG	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Philippines) en_PH	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2, City ZipCode State Country
English (Pakistan) en_PK	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City-ZipCode State Country
English (Rwanda) en_RW	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Solomon Islands) en_SB	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Seychelles) en_SC	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
English (Singapore) en_SG	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			State Country
English (St. Helena) en_SH	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Sierra Leone) en_SL	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Sierra Leone, SLL) en_SL_SLL	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Sint Maarten) en_SX	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Eswatini) en_SZ	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Tonga) en_TO	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Trinidad & Tobago) en_TT	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
English (Tanzania) en_TZ	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
English (Uganda) en_UG	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (United States) en_US	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Vanuatu) en_VU	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Samoa) en_WS	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (South Africa) en_ZA	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Español (Argentina) es_AR	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Español (Bolivia) es_BO	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			City, State ZipCode Country
Español (Chile) es_CL	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Español (Colombia) es_CO	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State, ZipCode Country
Español (Costa Rica) es_CR	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 State, City ZipCode Country
Español (Cuba) es_CU	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Español (República Dominicana) es_DO	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Español (Ecuador) es_EC	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Español (España) es_ES	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			Country
Español (Guatemala) es_GT	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode-City State Country
Español (Honduras) es_HN	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Español (México) es_MX	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City, State Country
Español (Nicaragua) es_NI	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City, State Country
Español (Panamá) es_PA	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
Español (Perú) es_PE	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Español (Puerto Rico) es_PR	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			State Country
Español (Paraguay) es_PY	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Español (El Salvador) es_SV	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode-City State Country
Español (Estados Unidos) es_US	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Español (Uruguay) es_UY	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Español (Venezuela) es_VE	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode, State Country
Eesti (Eesti) et_EE	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Euskara (Espainia) eu_ES	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
)) fa_IR	—	Ms. FName LName	State City

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			Address Line 1, Address Line 2 ZipCode Country
Suomi (Suomi) fi_FI	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Français (Belgique) fr_BE	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Français (Canada) fr_CA	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
Français (Suisse) fr_CH	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Français (France) fr_FR	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Français (Guinée) fr_GN	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Français (Haïti) fr_HT	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
Français (Comores) fr_KM	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Français (Luxembourg) fr_LU	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Français (Maroc) fr_MA	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Français (Monaco) fr_MC	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Français (Mauritanie) fr_MR	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Français (Wallis-et-Futuna) fr_WF	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Gaeilge (Éire) ga_IE	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
() gu_IN	12,34,567.567 -12,34,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			State Country
Ōlelo Hawai i (Amelika Hui Pū la) haw_US	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
() hi_IN	12,34,567.567 -12,34,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Hmong (United States) hmn_US	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Hrvatski (Hrvatska) hr_HR	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Hrvatski (Hrvatska, HRK) hr_HR_HRK	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Haitian Creole (Haiti) ht_HT	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Haitian Creole (United States) ht_US	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
Magyar (Magyarország) hu_HU	1 234 567,567 -1 234 567,567	LName FName	City Address Line 1, Address Line 2 ZipCode State Country
() hy_AM	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Indonesia (Indonesia) in_ID	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
Íslenska (Ísland) is_IS	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Italiano (Svizzera) it_CH	1'234'567.567 -1'234'567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Italiano (Italia) it_IT	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
)) iw_IL	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
日本語 (日本) ja_JP	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City State ZipCode Country
Yiddish (United States) ji_US	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
() ka_GE	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
аза тілі (аза стан) kk_KZ	1 234 567,567 -1 234 567,567	Ms. FName LName	ZipCode State City Address Line 1, Address Line 2 Country
Kalaallisut (Kalaallit Nunaat) kl_GL	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
() km_KH	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
() kn_IN	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
한국어 (북한) ko_KP	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
한국어 (대한민국) ko_KR	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
Kyrgyz (Kyrgyzstan) ky_KG	1 234 567,567 -1 234 567,567	Ms. FName LName	ZipCode City Address Line 1, Address Line 2 State Country
Lëtzebuergesch (Lëtzebuerg) lb_LU	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Lao (Laos) lo_LA	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Lietuvių (Lietuva) lt_LT	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Luba-Katanga (Congo - Kinshasa) lu_CD	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Latviešu (Latvija) lv_LV	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, ZipCode

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			State Country
Te reo (New Zealand) mi_NZ	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Македонски (Северна Македонија) mk_MK	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
() ml_IN	12,34,567.567 -12,34,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
() mr_IN	, , , . - , , , .	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Melayu (Brunei) ms_BN	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Melayu (Malaysia) ms_MY	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Malti (Malta) mt_MT	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
() my_MM	, , . - , , .	Ms. FName LName	Address Line 1, Address Line 2 City, ZipCode State Country
Nepali (Nepal) ne_NP	, , . - , , .	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Nederlands (Aruba) nl_AW	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Nederlands (België) nl_BE	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Nederlands (Nederland) nl_NL	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Nederlands (Suriname) nl_SR	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
Norsk (Norge) no_NO	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
() pa_IN	12,34,567.567 -12,34,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			State Country
Polski (Polska) pl_PL	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Pashto (Afghanistan) ps_AF	-	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Português (Angola) pt_AO	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Português (Brasil) pt_BR	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City-State ZipCode Country
Português (Cabo Verde) pt_CV	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Português (Moçambique) pt_MZ	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Português (Portugal) pt_PT	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			State Country
Português (São Tomé e Príncipe) pt_ST	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Rumantsch (Svizra) rm_CH	1'234'567.567 -1'234'567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Rundi (Burundi) rn_BI	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Română (Republica Moldova) ro_MD	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Română (România) ro_RO	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Русский (Армения) ru_AM	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Русский (Беларусь) ru_BY	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
Русский (Киргизия) ru_KG	1 234 567,567 -1 234 567,567	Ms. FName LName	ZipCode City Address Line 1, Address Line 2 State Country
Русский (Казахстан) ru_KZ	1 234 567,567 -1 234 567,567	Ms. FName LName	ZipCode State City Address Line 1, Address Line 2 Country
Русский (Литва) ru_LT	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Русский (Молдова) ru_MD	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Русский (Польша) ru_PL	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Русский (Россия) ru_RU	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
Русский (Украина) ru_UA	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City State

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			ZipCode Country
Serbian (Latin) (Bosnia and Herzegovina) sh_BA	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Serbian (Latin) (Serbia) sh_CS	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Montenegrin (Montenegro) sh_ME	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Montenegrin (Montenegro, USD) sh_ME_USD	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Slovenčina (Slovensko) sk_SK	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Slovenščina (Slovenija) sl_SI	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Samoan (United States) sm_US	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Samoan (Samoa) sm_WS	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			City, State ZipCode Country
Somali (Djibouti) so_DJ	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Somali (Somalia) so_SO	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Shqip (Shqipëri) sq_AL	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Serbian (Cyrillic) (Bosnia and Herzegovina) sr_BA	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Serbian (Cyrillic) (Serbia) sr_CS	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Српски (Србија) sr_RS	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Svenska (Sverige) sv_SE	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
Kiswahili (Kenya) sw_KE	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
() ta_IN	12,34,567.567 -12,34,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
() ta_LK	12,34,567.567 -12,34,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
() te_IN	12,34,567.567 -12,34,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Tajik (Tajikistan) tg_TJ	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
ไทย (ไทย) th_TH	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
Tigrinya (Ethiopia) ti_ET	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
Tagalog (Pilipinas) tl_PH	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2, City ZipCode State Country
Türkçe (Türkiye) tr_TR	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City/State Country
Українська (Україна) uk_UA	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
Urdu (Urdu) ur_PK	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City-ZipCode State Country
Uzbek (Latin, Uzbekistan) uz_LATN_UZ	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Tiếng Việt (Việt Nam) vi_VN	1.234.567,567 -1.234.567,567	LName FName	Address Line 1, Address Line 2 City State ZipCode Country
IsiXhosa (eMzantsi Afrika) xh_ZA	1 234 567.567 -1 234 567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
Yoruba (Benin) yo_BJ	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
中文 (中国) zh_CN	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
中文 (中国, CNH) zh_CN_CNH	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
中文 (中国, 拼音顺序) zh_CN_PINYIN	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
中文 (中国, 笔画顺序) zh_CN_STROKE	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
zh_HK	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
() zh_HK_STROKE	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
zh_MO	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
zh_MY	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 ZipCode City State Country
zh_SG	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City ZipCode State Country
中文 (台灣) zh_TW	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
中文 (台灣, 筆劃順序) zh_TW_STROKE	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
IsiZulu (iNingizimu Afrika) zu_ZA	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country

Supported Date and Time Formats (ICU)

The start day of the week and the International Components for Unicode (ICU) date and time formats for each Salesforce supported locale.

We use three variations of date and time formats across the Salesforce application: short, medium, and long. All three formats are listed for each locale by length, with the short format listed first. For unauthenticated guest users, date and time formats on Salesforce Sites are based on the user's browser settings instead of the user's personal locale.

 **Note:** The user's `Language` setting determines the language of the AM/PM designator in date/time fields. For example, if the user's language is English, times in the Chinese (Singapore) locale display with English AM/PM designators.

 **Note:** We recommend viewing this information in Salesforce Help. Not all characters appear correctly in PDFs.

EDITIONS

Available in: Lightning Experience and Salesforce Classic ([not available in all orgs](#))

Available in: **Group, Professional, Enterprise, Performance, Unlimited, Database.com,** and **Developer** Editions

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
Afrikaans (Suid-Afrika) af_ZA	2008-01-28 16:30 28 Jan. 2008 16:30:05 2008-01-28 16:30:05 GMT-8	16:30	Sunday – Saturday
() am_ET	28/01/2008 4:30 28 2008 4:30:05 28/01/2008 4:30:05 -8	4:30	Sunday – Saturday
)) ar_AE	// ,: / / , : : // , : : -	:	Saturday – Sunday
)) ar_BH	// ,: / / , : : // , : : -	:	Saturday – Sunday
)) ar_DZ	28 /1 /2008, 4:30 28 /01 /2008, 4:30:05 28 /1 /2008, 4:30:05 -8	4:30	Saturday – Sunday
)) ar_EG	// ,: / / , : : // , : : -	:	Saturday – Sunday
)) ar_IQ	// ,: / / , : :	:	Saturday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	// ,:: -		
)) ar_JO	// ,: // ,:: // ,:: -	:	Saturday – Sunday
)) ar_KW	// ,: // ,:: // ,:: -	:	Saturday – Sunday
)) ar_LB	// ,: // ,:: // ,:: -	:	Monday – Sunday
)) ar_LY	28 /1 /2008, 4:30 28 /01 /2008, 4:30:05 28 /1 /2008, 4:30:05 -8	4:30	Saturday – Sunday
)) ar_MA	28 /1 /2008, 16:30 28 /01 /2008, 16:30:05 28 /1 /2008, 16:30:05 -8	16:30	Monday – Sunday
)) ar_OM	// ,: // ,:: // ,:: -	:	Saturday – Sunday
)) ar_QA	// ,: // ,:: // ,:: -	:	Saturday – Sunday
)) ar_SA	// ,: // ,:: // ,:: -	:	Sunday – Saturday
)) ar_SD	// ,: // ,:: // ,:: -	:	Saturday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
)) ar_SY	// ,: // ,:: // ,:: -	:	Saturday – Sunday
)) ar_TN	28 /1 /2008, 4:30 28 /01 /2008, 4:30:05 28 /1 /2008, 4:30:05 -8	4:30	Monday – Sunday
)) ar_YE	// ,: // ,:: // ,:: -	:	Sunday – Saturday
Azerbaijani (Azerbaijan) az_AZ	28.01.2008 16:30 28 Jan 2008 16:30:05 28.01.2008 16:30:05 GMT-8	16:30	Monday – Sunday
Belarusian (Belarus) be_BY	28.01.2008, 16:30 28 Jan 2008 г., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Български (България) bg_BG	28.01.2008 г., 16:30 ч. 28.01.2008 г., 16:30:05 ч. 28.01.2008 г., 16:30:05 ч. Гринуич-8	16:30 ч.	Monday – Sunday
() bn_BD	// : PM , : : PM // : : PM GMT -	: PM	Sunday – Saturday
() bn_IN	// : PM , : : PM // : : PM GMT -	: PM	Sunday – Saturday
Bosanski (Bosna i Hercegovina) bs_BA	28. 1. 2008. 16:30 28. jan 2008. 16:30:05 28. 1. 2008. 16:30:05 GMT -8	16:30	Monday – Sunday
Català (Espanya) ca_ES	28/1/2008 16:30 28 de gen. 2008, 16:30:05	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28/1/2008 16:30:05 GMT-8		
Čeština (Česko) cs_CZ	28.01.2008 16:30 28. 1. 2008 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
Cymraeg (Y Deyrnas Unedig) cy_GB	28/01/2008 16:30 28 Ion 2008 16:30:05 28/01/2008 16:30:05 GMT-8	16:30	Monday – Sunday
Dansk (Danmark) da_DK	28.01.2008 16.30 28. jan. 2008 16.30.05 28.01.2008 16.30.05 GMT-8	16.30	Monday – Sunday
Deutsch (Österreich) de_AT	28.01.2008, 16:30 28.01.2008, 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Deutsch (Belgien) de_BE	28.01.2008, 16:30 28.01.2008, 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Deutsch (Schweiz) de_CH	28.01.2008, 16:30 28.01.2008, 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Deutsch (Deutschland) de_DE	28.01.2008, 16:30 28.01.2008, 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Deutsch (Luxemburg) de_LU	28.01.2008, 16:30 28.01.2008, 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Dzongkha (Bhutan) dz_BT	- - PM Jan : : PM - - : PM -	PM	Sunday – Saturday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
Ελληνικά (Κύπρος) el_CY	28/1/2008, 4:30 μ.μ. 28 Ιαν 2008, 4:30:05 μ.μ. 28/1/2008, 4:30:05 μ.μ. GMT-8	4:30 μ.μ.	Monday – Sunday
Ελληνικά (Ελλάδα) el_GR	28/1/2008, 4:30 μ.μ. 28 Ιαν 2008, 4:30:05 μ.μ. 28/1/2008, 4:30:05 μ.μ. GMT-8	4:30 μ.μ.	Monday – Sunday
English (United Arab Emirates) en_AE	28/01/2008, 4:30 PM 28 Jan 2008, 4:30:05 PM 28/01/2008, 4:30:05 PM GMT-8	4:30 PM	Saturday – Sunday
English (Antigua & Barbuda) en_AG	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (Australia) en_AU	28/1/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/1/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Barbados) en_BB	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Belgium) en_BE	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Bermuda) en_BM	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Bahamas) en_BS	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (Botswana) en_BW	28/01/2008, 16:30 28 Jan 2008, 16:30:05	16:30	Sunday – Saturday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28/01/2008, 16:30:05 GMT-8		
English (Belize) en_BZ	28/01/2008, 16:30 28-Jan-2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
English (Canada) en_CA	2008-01-28, 4:30 p.m. Jan 28, 2008, 4:30:05 p.m. 2008-01-28, 4:30:05 p.m. PST	4:30 p.m.	Sunday – Saturday
English (Cameroon) en_CM	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Cyprus) en_CY	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Germany) en_DE	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Eritrea) en_ER	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Fiji) en_FJ	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Falkland Islands) en_FK	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (United Kingdom) en_GB	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
English (Ghana) en_GH	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Gibraltar) en_GI	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Gambia) en_GM	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Guyana) en_GY	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Hong Kong SAR China) en_HK	28/1/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/1/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (Indonesia) en_ID	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
English (Ireland) en_IE	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Israel) en_IL	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
English (India) en_IN	28/01/2008, 4:30 pm 28-Jan-2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (Italy) en_IT	1/28/2008, 16:30 Jan 28, 2008, 16:30:05	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	1/28/2008, 16:30:05 PST		
English (Jamaica) en_JM	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (Kenya) en_KE	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
English (Cayman Islands) en_KY	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Liberia) en_LR	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Madagascar) en_MG	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Malta) en_MT	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
English (Mauritius) en_MU	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Malawi) en_MW	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Malaysia) en_MY	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
English (Namibia) en_NA	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Nigeria) en_NG	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Netherlands) en_NL	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (New Zealand) en_NZ	28/01/2008, 4:30 pm 28/01/2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Papua New Guinea) en_PG	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Philippines) en_PH	1/28/2008, 4:30 PM Jan 28, 2008, 4:30:05 PM 1/28/2008, 4:30:05 PM PST	4:30 PM	Sunday – Saturday
English (Pakistan) en_PK	28/01/2008, 4:30 pm 28-Jan-2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (Rwanda) en_RW	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Solomon Islands) en_SB	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Seychelles) en_SC	28/01/2008, 16:30 28 Jan 2008, 16:30:05	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28/01/2008, 16:30:05 GMT-8		
English (Singapore) en_SG	28/1/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/1/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (St. Helena) en_SH	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Sierra Leone) en_SL	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Sierra Leone, SLL) en_SL_SLL	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Sint Maarten) en_SX	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Eswatini) en_SZ	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Tonga) en_TO	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Trinidad & Tobago) en_TT	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (Tanzania) en_TZ	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
English (Uganda) en_UG	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (United States) en_US	1/28/2008, 4:30 PM Jan 28, 2008, 4:30:05 PM 1/28/2008, 4:30:05 PM PST	4:30 PM	Sunday – Saturday
English (Vanuatu) en_VU	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Samoa) en_WS	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (South Africa) en_ZA	2008/01/28, 16:30 28 Jan 2008, 16:30:05 2008/01/28, 16:30:05 GMT-8	16:30	Sunday – Saturday
Español (Argentina) es_AR	28/1/2008, 16:30 28 ene 2008 16:30:05 28/1/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Español (Bolivia) es_BO	28/1/2008, 16:30 28 ene de 2008 16:30:05 28/1/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Español (Chile) es_CL	28-01-2008, 16:30 28-01-2008 16:30:05 28-01-2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Español (Colombia) es_CO	28/01/2008, 4:30 p. m. 28/01/2008, 4:30:05 p. m. 28/01/2008, 4:30:05 p. m. GMT-8	4:30 p. m.	Sunday – Saturday
Español (Costa Rica) es_CR	28/1/2008, 16:30 28 ene 2008 16:30:05	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28/1/2008, 16:30:05 GMT-8		
Español (Cuba) es_CU	28/1/2008, 16:30 28 ene 2008 16:30:05 28/1/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Español (República Dominicana) es_DO	28/1/2008, 4:30 p. m. 28 ene 2008 4:30:05 p. m. 28/1/2008, 4:30:05 p. m. GMT-8	4:30 p. m.	Sunday – Saturday
Español (Ecuador) es_EC	28/1/2008, 16:30 28 ene 2008 16:30:05 28/1/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Español (España) es_ES	28/1/2008, 16:30 28 ene 2008, 16:30:05 28/1/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Español (Guatemala) es_GT	28/01/2008, 16:30 28/01/2008 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
Español (Honduras) es_HN	28/1/2008, 16:30 28 ene 2008 16:30:05 28/1/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
Español (México) es_MX	28/01/2008, 16:30 28 ene 2008 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
Español (Nicaragua) es_NI	28/1/2008, 16:30 28 ene 2008 16:30:05 28/1/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
Español (Panamá) es_PA	01/28/2008, 4:30 p. m. 01/28/2008 4:30:05 p. m. 01/28/2008, 4:30:05 p. m. GMT-8	4:30 p. m.	Sunday – Saturday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
Español (Perú) es_PE	28/01/2008, 16:30 28 ene. 2008 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
Español (Puerto Rico) es_PR	01/28/2008, 4:30 p. m. 01/28/2008 4:30:05 p. m. 01/28/2008, 4:30:05 p. m. GMT-8	4:30 p. m.	Sunday – Saturday
Español (Paraguay) es_PY	28/1/2008, 16:30 28 ene. 2008 16:30:05 28/1/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
Español (El Salvador) es_SV	28/1/2008, 16:30 28 ene 2008 16:30:05 28/1/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
Español (Estados Unidos) es_US	28/1/2008, 4:30 p. m. 28 ene 2008, 4:30:05 p. m. 28/1/2008, 4:30:05 p. m. PST	4:30 p. m.	Sunday – Saturday
Español (Uruguay) es_UY	28/1/2008, 16:30 28 ene. 2008 16:30:05 28/1/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Español (Venezuela) es_VE	28/1/2008, 4:30 p. m. 28 ene. 2008 4:30:05 p. m. 28/1/2008, 4:30:05 p. m. GMT-8	4:30 p. m.	Sunday – Saturday
Eesti (Eesti) et_EE	28.01.2008 16:30 28. jaan 2008 16:30:05 28.01.2008 16:30:05 GMT –8	16:30	Monday – Sunday
Euskara (Espainia) eu_ES	2008/1/28 16:30 2008(e)ko urt. 28(a) 16:30:05 2008/1/28 16:30:05 (PST)	16:30	Monday – Sunday
)) fa_IR	: // ::	:	Saturday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	:: // (-)		
Suomi (Suomi) fi_FI	28.1.2008 16:30 28.1.2008 klo 16:30:05 28.1.2008 16:30:05 UTC-8	16:30	Monday – Sunday
Français (Belgique) fr_BE	28/01/2008 16:30 28 janv. 2008, 16:30:05 28/01/2008 16:30:05 UTC-8	16:30	Monday – Sunday
Français (Canada) fr_CA	2008-01-28 16 h 30 28 janv. 2008, 16 h 30 min 05 s 2008-01-28 16 h 30 min 05 s HNP	16 h 30	Sunday – Saturday
Français (Suisse) fr_CH	28.01.2008 16:30 28 janv. 2008, 16:30:05 28.01.2008 16:30:05 UTC-8	16:30	Monday – Sunday
Français (France) fr_FR	28/01/2008 16:30 28 janv. 2008, 16:30:05 28/01/2008 16:30:05 UTC-8	16:30	Monday – Sunday
Français (Guinée) fr_GN	28/01/2008 16:30 28 janv. 2008, 16:30:05 28/01/2008 16:30:05 UTC-8	16:30	Monday – Sunday
Français (Haïti) fr_HT	28/01/2008 16:30 28 janv. 2008, 16:30:05 28/01/2008 16:30:05 UTC-8	16:30	Monday – Sunday
Français (Comores) fr_KM	28/01/2008 16:30 28 janv. 2008, 16:30:05 28/01/2008 16:30:05 UTC-8	16:30	Monday – Sunday
Français (Luxembourg) fr_LU	28/01/2008 16:30 28 janv. 2008, 16:30:05 28/01/2008 16:30:05 UTC-8	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
Français (Maroc) fr_MA	28/01/2008 16:30 28 jan. 2008, 16:30:05 28/01/2008 16:30:05 UTC-8	16:30	Monday – Sunday
Français (Monaco) fr_MC	28/01/2008 16:30 28 janv. 2008, 16:30:05 28/01/2008 16:30:05 UTC-8	16:30	Monday – Sunday
Français (Mauritanie) fr_MR	28/01/2008 4:30 PM 28 janv. 2008, 4:30:05 PM 28/01/2008 4:30:05 PM UTC-8	4:30 PM	Monday – Sunday
Français (Wallis-et-Futuna) fr_WF	28/01/2008 16:30 28 janv. 2008, 16:30:05 28/01/2008 16:30:05 UTC-8	16:30	Monday – Sunday
Gaeilge (Éire) ga_IE	28/01/2008 16:30 28 Ean 2008 16:30:05 28/01/2008 16:30:05 ACAC	16:30	Monday – Sunday
() gu_IN	28/1/2008 04:30 PM 28 , 2008 04:30:05 PM 28/1/2008 04:30:05 PM GMT-8	04:30 PM	Sunday – Saturday
Ōlelo Hawai i (Amelika Hui Pū la) haw_US	28/i/2008 4:30 PM 28 lan. 2008 4:30:05 PM 28/i/2008 4:30:05 PM GMT-8	4:30 PM	Sunday – Saturday
() hi_IN	28/1/2008, 4:30 pm 28 2008, 4:30:05 pm 28/1/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
Hmong (United States) hmn_US	1/28/2008, 4:30 PM Jan 28, 2008, 4:30:05 PM 1/28/2008, 4:30:05 PM PST	4:30 PM	Sunday – Saturday
Hrvatski (Hrvatska) hr_HR	28. 01. 2008. 16:30 28. sij 2008. 16:30:05	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28. 01. 2008. 16:30:05 GMT -8		
Hrvatski (Hrvatska, HRK) hr_HR_HRK	28. 01. 2008. 16:30 28. sij 2008. 16:30:05 28. 01. 2008. 16:30:05 GMT -8	16:30	Monday – Sunday
Haitian Creole (Haiti) ht_HT	1/28/2008, 16:30 Jan 28, 2008, 16:30:05 1/28/2008, 16:30:05 PST	16:30	Monday – Sunday
Haitian Creole (United States) ht_US	1/28/2008, 4:30 PM Jan 28, 2008, 4:30:05 PM 1/28/2008, 4:30:05 PM PST	4:30 PM	Sunday – Saturday
Magyar (Magyarország) hu_HU	2008. 01. 28. 16:30 2008. jan. 28. 16:30:05 2008. 01. 28. 16:30:05 GMT-8	16:30	Monday – Sunday
() hy_AM	28.01.2008, 16:30 28 , 2008 ., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Indonesia (Indonesia) in_ID	28/01/2008 16.30 28 Jan 2008 16.30.05 28/01/2008 16.30.05 PST	16.30	Sunday – Saturday
Íslenska (Ísland) is_IS	28.1.2008, 16:30 28. jan. 2008, 16:30:05 28.1.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Italiano (Svizzera) it_CH	28.01.2008, 16:30 28 gen 2008, 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Italiano (Italia) it_IT	28/01/2008, 16:30 28 gen 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
)) iw_IL	28.1.2008, 16:30 28 . 2008, 16:30:05 28.1.2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
日本語 (日本) ja_JP	2008/01/28 16:30 2008/01/28 16:30:05 2008/01/28 16:30:05 GMT-8	16:30	Sunday – Saturday
Yiddish (United States) ji_US	1/28/2008, 4:30 PM Jan 28, 2008, 4:30:05 PM 1/28/2008, 4:30:05 PM PST	4:30 PM	Sunday – Saturday
() ka_GE	28.01.2008, 16:30 28 . 2008, 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
аза тілі (аза стан) kk_KZ	28.01.2008, 16:30 2008 ж. 28 а., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Kalaallisut (Kalaallit Nunaat) kl_GL	2008-01-28 16.30 2008 jan 28 16.30.05 2008-01-28 16.30.05 GMT-8	16.30	Monday – Sunday
() km_KH	28/1/2008, 4:30 PM 28 . 2008, 4:30:05 PM 28/1/2008, 4:30:05 PM -8	4:30 PM	Sunday – Saturday
() kn_IN	28/1/2008 04:30 28, 2008 04:30:05 28/1/2008 04:30:05 GMT-8	04:30	Sunday – Saturday
한국어 (북한) ko_KP	2008. 1. 28. 오후 4:30 2008. 1. 28. 오후 4:30:05 2008. 1. 28. 오후 4:30:05 GMT-8	오후 4:30	Monday – Sunday
한국어 (대한민국)	2008. 1. 28. 오후 4:30	오후 4:30	Sunday – Saturday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
ko_KR	2008. 1. 28. 오후 4:30:05 2008. 1. 28. 오후 4시 30분 5초 GMT-8		
Kyrgyz (Kyrgyzstan) ky_KG	28/1/2008 16:30 2008-ж., 28-Jan 16:30:05 28/1/2008 16:30:05 GMT-8	16:30	Monday – Sunday
Lëtzebuergesch (Lëtzebuerg) lb_LU	28.01.2008 16:30 28. Jan. 2008 16:30:05 28.01.2008 16:30:05 GMT-8	16:30	Monday – Sunday
Lao (Laos) lo_LA	28/1/2008, 16:30 28 Jan 2008, 16:30:05 28/1/2008, 16 30 05 GMT-8	16:30	Sunday – Saturday
Lietuvių (Lietuva) lt_LT	2008-01-28 16:30 2008-01-28 16:30:05 2008-01-28 16:30:05 GMT-8	16:30	Monday – Sunday
Luba-Katanga (Congo - Kinshasa) lu_CD	28/1/2008 16:30 28 Jan 2008 16:30:05 28/1/2008 16:30:05 GMT-8	16:30	Monday – Sunday
Latviešu (Latvija) lv_LV	28.01.2008 16:30 2008. gada 28. janv. 16:30:05 28.01.2008 16:30:05 GMT-8	16:30	Monday – Sunday
Te reo (New Zealand) mi_NZ	28-01-2008 4:30 PM 28 Kohi 2008 4:30:05 PM 28-01-2008 4:30:05 PM GMT-8	4:30 PM	Monday – Sunday
Македонски (Северна Македонија) mk_MK	28.1.2008, во 16:30 28.1.2008, во 16:30:05 28.1.2008, во 16:30:05 GMT-8	16:30	Monday – Sunday
() ml_IN	28/1/2008 4:30 PM 2008, 28 4:30:05 PM	4:30 PM	Sunday – Saturday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28/1/2008 4:30:05 PM -8		
() mr_IN	// , : PM , , : : PM // , : : PM [GMT]-	: PM	Sunday – Saturday
Melayu (Brunei) ms_BN	28/01/2008, 4:30 PTG 28 Jan 2008, 4:30:05 PTG 28/01/2008, 4:30:05 PTG GMT-8	4:30 PTG	Monday – Sunday
Melayu (Malaysia) ms_MY	28/01/2008, 4:30 PTG 28 Jan 2008, 4:30:05 PTG 28/01/2008, 4:30:05 PTG GMT-8	4:30 PTG	Monday – Sunday
Malti (Malta) mt_MT	28/01/2008 16:30 28 Jan 2008 16:30:05 28/01/2008 16:30:05 GMT-8	16:30	Sunday – Saturday
() my_MM	- - : - : : - - GMT- : :	:	Sunday – Saturday
Nepali (Nepal) ne_NP	// , : Jan , : : // , : : GMT-	:	Sunday – Saturday
Nederlands (Aruba) nl_AW	28-01-2008 16:30 28 jan. 2008 16:30:05 28-01-2008 16:30:05 PST	16:30	Monday – Sunday
Nederlands (België) nl_BE	28/01/2008 16:30 28 jan. 2008 16:30:05 28/01/2008 16:30:05 PST	16:30	Monday – Sunday
Nederlands (Nederland) nl_NL	28-01-2008 16:30 28 jan. 2008 16:30:05 28-01-2008 16:30:05 PST	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
Nederlands (Suriname) nl_SR	28-01-2008 16:30 28 jan. 2008 16:30:05 28-01-2008 16:30:05 PST	16:30	Monday – Sunday
Norsk (Norge) no_NO	28.01.2008, 16:30 28. jan. 2008, 16:30:05 28.01.2008, 16:30:05 PST	16:30	Monday – Sunday
() pa_IN	28/1/2008, 4:30 . . 28 2008, 4:30:05 . . 28/1/2008, 4:30:05 . . GMT-8	4:30 . .	Sunday – Saturday
Polski (Polska) pl_PL	28.01.2008, 16:30 28 sty 2008, 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Pashto (Afghanistan) ps_AF	B : / / BC Nov : : B : : / / (GMT-)	:	Saturday – Sunday
Português (Angola) pt_AO	28/01/2008, 16:30 28/01/2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Português (Brasil) pt_BR	28/01/2008 16:30 28 de jan. de 2008 16:30:05 28/01/2008 16:30:05 GMT-8	16:30	Sunday – Saturday
Português (Cabo Verde) pt_CV	28/01/2008, 16:30 28/01/2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Português (Moçambique) pt_MZ	28/01/2008, 16:30 28/01/2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
Português (Portugal) pt_PT	28/01/2008, 16:30 28/01/2008, 16:30:05	16:30	Sunday – Saturday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28/01/2008, 16:30:05 GMT-8		
Português (São Tomé e Príncipe) pt_ST	28/01/2008, 16:30 28/01/2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Rumantsch (Svizra) rm_CH	28-01-2008 16:30 28-01-2008 16:30:05 28-01-2008 16:30:05 GMT-8	16:30	Monday – Sunday
Rundi (Burundi) rn_BI	28/1/2008 16:30 28 Jan 2008 16:30:05 28/1/2008 16:30:05 GMT-8	16:30	Monday – Sunday
Română (Republica Moldova) ro_MD	28.01.2008, 16:30 28 ian. 2008, 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Română (România) ro_RO	28.01.2008, 16:30 28 ian. 2008, 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Русский (Армения) ru_AM	28.01.2008, 16:30 28 янв. 2008 г., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Русский (Беларусь) ru_BY	28.01.2008, 16:30 28 янв. 2008 г., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Русский (Киргизия) ru_KG	28.01.2008, 16:30 28 янв. 2008 г., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Русский (Казахстан) ru_KZ	28.01.2008, 16:30 28 янв. 2008 г., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
Русский (Литва) ru_LT	28.01.2008, 16:30 28 янв. 2008 г., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Русский (Молдова) ru_MD	28.01.2008, 16:30 28 янв. 2008 г., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Русский (Польша) ru_PL	28.01.2008, 16:30 28 янв. 2008 г., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Русский (Россия) ru_RU	28.01.2008, 16:30 28 янв. 2008 г., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Русский (Украина) ru_UA	28.01.2008, 16:30 28 янв. 2008 г., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Serbian (Latin) (Bosnia and Herzegovina) sh_BA	28.1.2008. 16:30 28. 1. 2008. 16:30:05 28.1.2008. 16:30:05 GMT-8	16:30	Monday – Sunday
Serbian (Latin) (Serbia) sh_CS	28.1.2008. 16:30 28. 1. 2008. 16:30:05 28.1.2008. 16:30:05 GMT-8	16:30	Monday – Sunday
Montenegrin (Montenegro) sh_ME	28.1.2008. 16:30 28. 1. 2008. 16:30:05 28.1.2008. 16:30:05 GMT-8	16:30	Monday – Sunday
Montenegrin (Montenegro, USD) sh_ME_USD	28.1.2008. 16:30 28. 1. 2008. 16:30:05 28.1.2008. 16:30:05 GMT-8	16:30	Monday – Sunday
Slovenčina (Slovensko) sk_SK	28. 1. 2008 16:30 28. 1. 2008, 16:30:05	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28. 1. 2008 16:30:05 GMT-8		
Slovenščina (Slovenija) sl_SI	28. 01. 2008, 16:30 28. jan. 2008, 16:30:05 28. 01. 2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Samoan (United States) sm_US	1/28/2008, 4:30 PM Jan 28, 2008, 4:30:05 PM 1/28/2008, 4:30:05 PM PST	4:30 PM	Sunday – Saturday
Samoan (Samoa) sm_WS	1/28/2008, 4:30 PM Jan 28, 2008, 4:30:05 PM 1/28/2008, 4:30:05 PM PST	4:30 PM	Sunday – Saturday
Somali (Djibouti) so_DJ	28/01/2008 4:30 PM 28-Jan-2008 ee 4:30:05 PM 28/01/2008 4:30:05 PM GMT-8	4:30 PM	Saturday – Sunday
Somali (Somalia) so_SO	28/01/2008 4:30 PM 28-Jan-2008 ee 4:30:05 PM 28/01/2008 4:30:05 PM GMT-8	4:30 PM	Monday – Sunday
Shqip (Shqipëri) sq_AL	28.1.2008, 4:30 e pasdites 28 jan 2008, 4:30:05 e pasdites 28.1.2008, 4:30:05 e pasdites, GMT-8	4:30 e pasdites	Monday – Sunday
Serbian (Cyrillic) (Bosnia and Herzegovina) sr_BA	28.1.2008. 16:30 28. 1. 2008. 16:30:05 28.1.2008. 16:30:05 GMT-8	16:30	Monday – Sunday
Serbian (Cyrillic) (Serbia) sr_CS	28.1.2008. 16:30 28. 1. 2008. 16:30:05 28.1.2008. 16:30:05 GMT-8	16:30	Monday – Sunday
Српски (Србија) sr_RS	28.1.2008. 16:30 28. 1. 2008. 16:30:05 28.1.2008. 16:30:05 GMT-8	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
Svenska (Sverige) sv_SE	2008-01-28 16:30 28 jan. 2008 16:30:05 2008-01-28 16:30:05 GMT-8	16:30	Monday – Sunday
Kiswahili (Kenya) sw_KE	28/01/2008 16:30 28 Jan 2008 16:30:05 28/01/2008 16:30:05 GMT -8	16:30	Sunday – Saturday
() ta_IN	28/1/2008, 4:30 28 ., 2008, 4:30:05 28/1/2008, 4:30:05 GMT-8	4:30	Sunday – Saturday
() ta_LK	28/1/2008, 16:30 28 ., 2008, 16:30:05 28/1/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
() te_IN	28-01-2008 4:30 PM 28 , 2008 4:30:05 PM 28-01-2008 4:30:05 PM GMT-8	4:30 PM	Sunday – Saturday
Tajik (Tajikistan) tg_TJ	28/01/2008 16:30 28 Jan 2008 16:30:05 28/01/2008 16:30:05 GMT-8	16:30	Monday – Sunday
ไทย (ไทย) th_TH	28/1/2551 16:30 28 ม.ค. 2551 16:30:05 28/1/2551 16 นาฬิกา 30 นาที 05 วินาที GMT-8	16:30	Sunday – Saturday
Tigrinya (Ethiopia) ti_ET	28/01/2008 4:30 PM 28 Jan 2008 4:30:05 PM 28/01/2008 4:30:05 PM GMT-8	4:30 PM	Sunday – Saturday
Tagalog (Pilipinas) tl_PH	1/28/2008, 4:30 PM Ene 28, 2008, 4:30:05 PM 1/28/2008, 4:30:05 PM GMT-8	4:30 PM	Sunday – Saturday
Türkçe (Türkiye) tr_TR	28.01.2008 16:30 28 Oca 2008 16:30:05	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28.01.2008 16:30:05 GMT-8		
Українська (Україна) uk_UA	28.01.2008, 16:30 28 січ. 2008 р., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
)) ur_PK	28/1/2008 4:30 PM 28 2008 4:30:05 PM 28/1/2008 4:30:05 PM GMT -8	4:30 PM	Sunday – Saturday
Uzbek (Latin, Uzbekistan) uz_LATN_UZ	28/01/2008, 16:30 28-Jan, 2008, 16:30:05 28/01/2008, 16:30:05 (GMT-8)	16:30	Monday – Sunday
Ti ng Vi t (Vi t Nam) vi_VN	16:30, 28/01/2008 16:30:05, 28 thg 1, 2008 16:30:05 PST, 28/01/2008	16:30	Monday – Sunday
IsiXhosa (eMzantsi Afrika) xh_ZA	2008-01-28 16:30 2008 Jan 28 16:30:05 2008-01-28 16:30:05 GMT-8	16:30	Sunday – Saturday
Yoruba (Benin) yo_BJ	28/1/2008 16:30 28 01 2008 16:30:05 28/1/2008 16:30:05 WAT-8	16:30	Monday – Sunday
中文 (中国) zh_CN	2008/1/28 16:30 2008年1月28日 16:30:05 2008/1/28 GMT-8 16:30:05	16:30	Sunday – Saturday
中文 (中国, CNH) zh_CN_CNH	2008/1/28 16:30 2008年1月28日 16:30:05 2008/1/28 GMT-8 16:30:05	16:30	Sunday – Saturday
中文 (中国, 拼音顺序) zh_CN_PINYIN	2008/1/28 16:30 2008年1月28日 16:30:05 2008/1/28 GMT-8 16:30:05	16:30	Sunday – Saturday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
中文（中国，笔画顺序） zh_CN_STROKE	2008/1/28 16:30 2008年1月28日 16:30:05 2008/1/28 GMT-8 16:30:05	16:30	Sunday – Saturday
zh_HK	28/1/2008 4:30 2008 1 28 4:30:05 28/1/2008 4:30:05 [PST]	4:30	Sunday – Saturday
() zh_HK_STROKE	28/1/2008 4:30 2008 1 28 4:30:05 28/1/2008 4:30:05 [PST]	4:30	Sunday – Saturday
zh_MO	28/1/2008 4:30 2008 1 28 4:30:05 28/1/2008 4:30:05 [PST]	4:30	Sunday – Saturday
zh_MY	2008/1/28 4:30 2008 1 28 4:30:05 2008/1/28 GMT-8 4:30:05	4:30	Monday – Sunday
zh_SG	28/01/2008 4:30 2008 1 28 4:30:05 28/01/2008 GMT-8 4:30:05	4:30	Sunday – Saturday
中文（台灣） zh_TW	2008/1/28 下午4:30 2008年1月28日 下午4:30:05 2008/1/28 下午4:30:05 [PST]	下午4:30	Sunday – Saturday
中文（台灣，筆劃順序） zh_TW_STROKE	2008/1/28 下午4:30 2008年1月28日 下午4:30:05 2008/1/28 下午4:30:05 [PST]	下午4:30	Sunday – Saturday
IsiZulu (iNingizimu Afrika) zu_ZA	1/28/2008 16:30 Jan 28, 2008 16:30:05 1/28/2008 16:30:05 GMT-8	16:30	Sunday – Saturday

[Supported Currencies \(ICU\)](#)

Salesforce supported currencies, listed by locale with International Components for Unicode (ICU) formats.

Supported Currencies (ICU)

Salesforce supported currencies, listed by locale with International Components for Unicode (ICU) formats.

 **Note:** We recommend viewing this information in Salesforce Help. Not all characters appear correctly in PDFs.

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
Afrikaans (Suid-Afrika) af_ZA	South African Rand	ZAR	R 1 234 567,57 -R 1 234 567,57
() am_ET	Ethiopian Birr	ETB	1,234,567.57 - 1,234,567.57
)) ar_AE		AED	.. - ..
)) ar_BH		BHD	.. - ..
)) ar_DZ		DZD	.. 1.234.567,57 -.. 1.234.567,57
)) ar_EG		EGP	.. - ..
)) ar_IQ		IQD	.. - ..
)) ar_JO		JOD	.. - ..
)) ar_KW		KWD	.. - ..
)) ar_LB		LBP	.. - ..

EDITIONS

Available in: Lightning Experience and Salesforce Classic ([not available in all orgs](#))

Available in: **Group, Professional, Enterprise, Performance, Unlimited, Database.com,** and **Developer** Editions

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
)) ar_LY		LYD	.. 1.234.567,57 -.. 1.234.567,57
)) ar_MA		MAD	.. 1.234.567,57 -.. 1.234.567,57
)) ar_OM		OMR	.. - ..
)) ar_QA		QAR	.. - ..
)) ar_SA		SAR	.. - ..
)) ar_SD		SDG	.. - ..
)) ar_SY		SYP	.. - ..
)) ar_TN		TND	.. 1.234.567,57 -.. 1.234.567,57
)) ar_YE		YER	.. - ..
Azerbaijani (Azerbaijan) az_AZ	Azerbaijan Manat	AZN	1.234.567,57 -1.234.567,57
Belarusian (Belarus) be_BY	Belarusian Ruble	BYN	1 234 567,57 Br -1 234 567,57 Br
Български (България) bg_BG	Български лев	BGN	1234567,57 лв. -1234567,57 лв.
() bn_BD	Bangladesh Taka	BDT	, , , - , , ,

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
() bn_IN	Indian Rupee	INR	, , . - , , .
Bosanski (Bosna i Hercegovina) bs_BA	Convertible Marks	BAM	1.234.567,57 KM -1.234.567,57 KM
Català (Espanya) ca_ES	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Čeština (Česko) cs_CZ	Česká koruna	CZK	1 234 567,57 Kč -1 234 567,57 Kč
Cymraeg (Y Deyrnas Unedig) cy_GB	British Pound	GBP	£1,234,567.57 -£1,234,567.57
Dansk (Danmark) da_DK	Krone, Danmark	DKK	1.234.567,57 kr. -1.234.567,57 kr.
Deutsch (Österreich) de_AT	Euro	EUR	€ 1.234.567,57 -€ 1.234.567,57
Deutsch (Belgien) de_BE	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Deutsch (Schweiz) de_CH	Schweizer Franken	CHF	CHF 1'234'567.57 CHF-1'234'567.57
Deutsch (Deutschland) de_DE	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Deutsch (Luxemburg) de_LU	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Dzongkha (Bhutan) dz_BT	Bhutan Ngultrum	BTN	Nu. , , . -Nu. , , .
Ελληνικά (Κύπρος) el_CY	Ευρώ	EUR	1.234.567,57 € -1.234.567,57 €

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
Ελληνικά (Ελλάδα) el_GR	Ευρώ	EUR	1.234.567,57 € -1.234.567,57 €
English (United Arab Emirates) en_AE	UAE Dirham	AED	AED 1,234,567.57 -AED 1,234,567.57
English (Antigua & Barbuda) en_AG	East Caribbean Dollar	XCD	\$1,234,567.57 -\$1,234,567.57
English (Australia) en_AU	Australian Dollar	AUD	\$1,234,567.57 -\$1,234,567.57
English (Barbados) en_BB	Barbados Dollar	BBD	\$1,234,567.57 -\$1,234,567.57
English (Belgium) en_BE	Euro	EUR	€1,234,567.57 -€1,234,567.57
English (Bermuda) en_BM	Bermuda Dollar	BMD	\$1,234,567.57 -\$1,234,567.57
English (Bahamas) en_BS	Bahamian Dollar	BSD	\$1,234,567.57 -\$1,234,567.57
English (Botswana) en_BW	Botswana Pula	BWP	P 1,234,567.57 -P 1,234,567.57
English (Belize) en_BZ	Belize Dollar	BZD	\$1,234,567.57 -\$1,234,567.57
English (Canada) en_CA	Canadian Dollar	CAD	\$1,234,567.57 -\$1,234,567.57
English (Cameroon) en_CM	CFA Franc (BEAC)	XAF	FCFA 1,234,567.57 -FCFA 1,234,567.57
English (Cyprus) en_CY	Euro	EUR	€1,234,567.57 -€1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
English (Germany) en_DE	Euro	EUR	€1,234,567.57 -€1,234,567.57
English (Eritrea) en_ER	Eritrea Nakfa	ERN	Nfk 1,234,567.57 -Nfk 1,234,567.57
English (Fiji) en_FJ	Fiji Dollar	FJD	\$1,234,567.57 -\$1,234,567.57
English (Falkland Islands) en_FK	Falkland Islands Pound	FKP	£1,234,567.57 -£1,234,567.57
English (United Kingdom) en_GB	British Pound	GBP	£1,234,567.57 -£1,234,567.57
English (Ghana) en_GH	Ghanaian Cedi	GHS	GH 1,234,567.57 -GH 1,234,567.57
English (Gibraltar) en_GI	Gibraltar Pound	GIP	£1,234,567.57 -£1,234,567.57
English (Gambia) en_GM	Gambian Dalasi	GMD	D 1,234,567.57 -D 1,234,567.57
English (Guyana) en_GY	Guyana Dollar	GYD	\$1,234,567.57 -\$1,234,567.57
English (Hong Kong SAR China) en_HK	Hong Kong Dollar	HKD	HK\$1,234,567.57 -HK\$1,234,567.57
English (Indonesia) en_ID	Indonesian Rupiah	IDR	IDR 1,234,567.57 -IDR 1,234,567.57
English (Ireland) en_IE	Euro	EUR	€1,234,567.57 -€1,234,567.57
English (Israel) en_IL	Israeli Shekel	ILS	1,234,567.57 -1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
English (India) en_IN	Indian Rupee	INR	12,34,567.57 - 12,34,567.57
English (Italy) en_IT	Euro	EUR	€1,234,567.57 -€1,234,567.57
English (Jamaica) en_JM	Jamaican Dollar	JMD	\$1,234,567.57 -\$1,234,567.57
English (Kenya) en_KE	Kenyan Shilling	KES	Ksh 1,234,567.57 -Ksh 1,234,567.57
English (Cayman Islands) en_KY	Cayman Islands Dollar	KYD	\$1,234,567.57 -\$1,234,567.57
English (Liberia) en_LR	Liberian Dollar	LRD	\$1,234,567.57 -\$1,234,567.57
English (Madagascar) en_MG	Malagasy Ariary	MGA	Ar 1,234,567.57 -Ar 1,234,567.57
English (Malta) en_MT	Euro	EUR	€1,234,567.57 -€1,234,567.57
English (Mauritius) en_MU	Mauritius Rupee	MUR	Rs 1,234,567.57 -Rs 1,234,567.57
English (Malawi) en_MW	Malawi Kwacha	MWK	MK 1,234,567.57 -MK 1,234,567.57
English (Malaysia) en_MY	Malaysian Ringgit	MYR	RM 1,234,567.57 -RM 1,234,567.57
English (Namibia) en_NA	Namibian Dollar	NAD	\$1,234,567.57 -\$1,234,567.57
English (Nigeria) en_NG	Nigerian Naira	NGN	1,234,567.57 - 1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
English (Netherlands) en_NL	Euro	EUR	€1,234,567.57 -€1,234,567.57
English (New Zealand) en_NZ	New Zealand Dollar	NZD	\$1,234,567.57 -\$1,234,567.57
English (Papua New Guinea) en_PG	Papua New Guinea Kina	PGK	K 1,234,567.57 -K 1,234,567.57
English (Philippines) en_PH	Philippine Peso	PHP	1,234,567.57 - 1,234,567.57
English (Pakistan) en_PK	Pakistani Rupee	PKR	Rs 1,234,567.57 -Rs 1,234,567.57
English (Rwanda) en_RW	Rwanda Franc	RWF	RF 1,234,567.57 -RF 1,234,567.57
English (Solomon Islands) en_SB	Solomon Islands Dollar	SBD	\$1,234,567.57 -\$1,234,567.57
English (Seychelles) en_SC	Seychelles Rupee	SCR	SR 1,234,567.57 -SR 1,234,567.57
English (Singapore) en_SG	Singapore Dollar	SGD	\$1,234,567.57 -\$1,234,567.57
English (St. Helena) en_SH	St Helena Pound	SHP	£1,234,567.57 -£1,234,567.57
English (Sierra Leone) en_SL	Sierra Leone Leone	SLE	SLE 1,234,567.57 -SLE 1,234,567.57
English (Sierra Leone, SLL) en_SL_SLL	Sierra Leone Leone	SLL	Le 1,234,567.57 -Le 1,234,567.57
English (Sint Maarten) en_SX	Neth Antilles Guilder	ANG	NAf. 1,234,567.57 -NAf. 1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
English (Eswatini) en_SZ	Eswatini Lilageni	SZL	E 1,234,567.57 -E 1,234,567.57
English (Tonga) en_TO	Tonga Pa'anga	TOP	T\$1,234,567.57 -T\$1,234,567.57
English (Trinidad & Tobago) en_TT	Trinidad&Tobago Dollar	TTD	\$1,234,567.57 -\$1,234,567.57
English (Tanzania) en_TZ	Tanzanian Shilling	TZS	TSh 1,234,567.57 -TSh 1,234,567.57
English (Uganda) en_UG	Ugandan Shilling	UGX	USh 1,234,567.57 -USh 1,234,567.57
English (United States) en_US	U.S. Dollar	USD	\$1,234,567.57 -\$1,234,567.57
English (Vanuatu) en_VU	Vanuatu Vatu	VUV	VT 1,234,567.57 -VT 1,234,567.57
English (Samoa) en_WS	Samoa Tala	WST	WS\$1,234,567.57 -WS\$1,234,567.57
English (South Africa) en_ZA	South African Rand	ZAR	R 1 234 567,57 -R 1 234 567,57
Español (Argentina) es_AR	Peso argentino	ARS	\$ 1.234.567,57 -\$ 1.234.567,57
Español (Bolivia) es_BO	Boliviano de Bolivia	BOB	Bs 1.234.567,57 -Bs 1.234.567,57
Español (Chile) es_CL	Peso chileno	CLP	\$1.234.567,57 -\$1.234.567,57
Español (Colombia) es_CO	Peso colombiano	COP	\$ 1.234.567,57 -\$ 1.234.567,57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
Español (Costa Rica) es_CR	Colón costarricense	CRC	1 234 567,57 - 1 234 567,57
Español (Cuba) es_CU	Peso cubano	CUP	\$1,234,567.57 -\$1,234,567.57
Español (República Dominicana) es_DO	Peso dominicano	DOP	RD\$1,234,567.57 -RD\$1,234,567.57
Español (Ecuador) es_EC	Dólar estadounidense	USD	\$1.234.567,57 \$-1.234.567,57
Español (España) es_ES	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Español (Guatemala) es_GT	Quetzal guatemalteco	GTQ	Q 1,234,567.57 -Q 1,234,567.57
Español (Honduras) es_HN	Lempira hondureño	HNL	L 1,234,567.57 -L 1,234,567.57
Español (México) es_MX	Peso mexicano	MXN	\$1,234,567.57 -\$1,234,567.57
Español (Nicaragua) es_NI	Córdoba nicaragüense	NIO	C\$1,234,567.57 -C\$1,234,567.57
Español (Panamá) es_PA	Balboa panameño	PAB	B/. 1,234,567.57 -B/. 1,234,567.57
Español (Perú) es_PE	Sol peruano	PEN	S/ 1,234,567.57 -S/ 1,234,567.57
Español (Puerto Rico) es_PR	Dólar estadounidense	USD	\$1,234,567.57 -\$1,234,567.57
Español (Paraguay) es_PY	Guaraní paraguayo	PYG	Gs. 1.234.567,57 Gs. -1.234.567,57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
Español (El Salvador) es_SV	Dólar estadounidense	USD	\$1,234,567.57 -\$1,234,567.57
Español (Estados Unidos) es_US	Dólar estadounidense	USD	\$1,234,567.57 -\$1,234,567.57
Español (Uruguay) es_UY	Peso uruguayo	UYU	\$ 1.234.567,57 -\$ 1.234.567,57
Español (Venezuela) es_VE	Bolívar soberano venezolano	VES	Bs.S 1.234.567,57 Bs.S-1.234.567,57
Eesti (Eesti) et_EE	Euro	EUR	1 234 567,57 € -1 234 567,57 €
Euskara (Espainia) eu_ES	Euro	EUR	1.234.567,57 € -1.234.567,57 €
فارسی (ایران) fa_IR	Iranian Rial	IRR	—
Suomi (Suomi) fi_FI	Euro	EUR	1 234 567,57 € -1 234 567,57 €
Français (Belgique) fr_BE	Euro	EUR	1 234 567,57 € -1 234 567,57 €
Français (Canada) fr_CA	Dollar canadien	CAD	1 234 567,57 \$ -1 234 567,57 \$
Français (Suisse) fr_CH	Franc suisse	CHF	1 234 567.57 CHF -1 234 567.57 CHF
Français (France) fr_FR	Euro	EUR	1 234 567,57 € -1 234 567,57 €
Français (Guinée) fr_GN	Franc guinéen	GNF	1 234 567,57 FG -1 234 567,57 FG

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
Français (Haïti) fr_HT	Gourde Haïtienne	HTG	1 234 567,57 G -1 234 567,57 G
Français (Comores) fr_KM	Franc comorien	KMF	1 234 567,57 CF -1 234 567,57 CF
Français (Luxembourg) fr_LU	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Français (Maroc) fr_MA	Dirham marocain	MAD	1.234.567,57 MAD -1.234.567,57 MAD
Français (Monaco) fr_MC	Euro	EUR	1 234 567,57 € -1 234 567,57 €
Français (Mauritanie) fr_MR	Ougulya mauritanien	MRU	1 234 567,57 UM -1 234 567,57 UM
Français (Wallis-et-Futuna) fr_WF	Franc du Pacifique	XPF	1 234 567,57 FCFP -1 234 567,57 FCFP
Gaeilge (Éire) ga_IE	Euro	EUR	€1,234,567.57 -€1,234,567.57
() gu_IN	Indian Rupee	INR	12,34,567.57 - 12,34,567.57
Ōlelo Hawai i (Amelika Hui Pū la) haw_US	U.S. Dollar	USD	\$1,234,567.57 -\$1,234,567.57
() hi_IN	Indian Rupee	INR	12,34,567.57 - 12,34,567.57
Hmong (United States) hmn_US	U.S. Dollar	USD	\$1,234,567.57 -\$1,234,567.57
Hrvatski (Hrvatska) hr_HR	ero	EUR	1.234.567,57 EUR -1.234.567,57 EUR

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
Hrvatski (Hrvatska, HRK) hr_HR_HRK	kuna	HRK	1.234.567,57 kn -1.234.567,57 kn
Haitian Creole (Haiti) ht_HT	Gourde Haïtienne	HTG	HTG 1,234,567.57 -HTG 1,234,567.57
Haitian Creole (United States) ht_US	Dollar américain	USD	\$1,234,567.57 -\$1,234,567.57
Magyar (Magyarország) hu_HU	Magyar forint	HUF	1 234 567,57 Ft -1 234 567,57 Ft
() hy_AM	Armenian Dram	AMD	1 234 567,57 -1 234 567,57
Indonesia (Indonesia) in_ID	Rupiah Indonesia	IDR	Rp 1.234.567,57 -Rp 1.234.567,57
Íslenska (Ísland) is_IS	Iceland Krona	ISK	1.234.567,57 ISK -1.234.567,57 ISK
Italiano (Svizzera) it_CH	Franco (Svizzero)	CHF	CHF 1'234'567.57 CHF-1'234'567.57
Italiano (Italia) it_IT	Euro	EUR	1.234.567,57 € -1.234.567,57 €
)) iw_IL		ILS	1,234,567.57 -1,234,567.57
日本語 (日本) ja_JP	日本円	JPY	¥ 1,234,567.57 - ¥ 1,234,567.57
Yiddish (United States) ji_US	U.S. Dollar	USD	\$1,234,567.57 -\$1,234,567.57
() ka_GE	Georgia Lari	GEL	1 234 567,57 -1 234 567,57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
аза тілі (азастан) kk_KZ	Kazakhstan Tenge	KZT	1 234 567,57 -1 234 567,57
Kalaallisut (Kalaallit Nunaat) kl_GL	Danish Krone	DKK	kr. 1.234.567,57 kr.-1.234.567,57
() km_KH	Cambodia Riel	KHR	1.234.567,57 -1.234.567,57
() kn_IN	Indian Rupee	INR	1,234,567.57 - 1,234,567.57
한국어 (북한) ko_KP	조선민주주의인민공화국 원	KPW	KPW 1,234,567.57 -KPW 1,234,567.57
한국어 (대한민국) ko_KR	대한민국 원	KRW	₩1,234,567.57 -₩1,234,567.57
Kyrgyz (Kyrgyzstan) ky_KG	Kyrgyzstan Som	KGS	1 234 567,57 com -1 234 567,57 com
Lëtzebuergesch (Lëtzebuerg) lb_LU	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Lao (Laos) lo_LA	Lao Kip	LAK	1.234.567,57 -1.234.567,57
Lietuvių (Lietuva) lt_LT	Euro	EUR	1 234 567,57 € -1 234 567,57 €
Luba-Katanga (Congo - Kinshasa) lu_CD	Franc Congolais	CDF	1.234.567,57 FC -1.234.567,57 FC
Latviešu (Latvija) lv_LV	Euro	EUR	1 234 567,57 € -1 234 567,57 €
Te reo (New Zealand) mi_NZ	New Zealand Dollar	NZD	\$ 1,234,567.57 -\$ 1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
Македонски (Северна Македонија) mk_MK	Macedonian Denar	MKD	1.234.567,57 ден. -1.234.567,57 ден.
() ml_IN	Indian Rupee	INR	1,234,567.57 - 1,234,567.57
() mr_IN	Indian Rupee	INR	, , . - , , .
Melayu (Brunei) ms_BN	Dolar Brunei	BND	\$ 1.234.567,57 -\$ 1.234.567,57
Melayu (Malaysia) ms_MY	Ringgit Malaysia	MYR	RM 1,234,567.57 -RM 1,234,567.57
Malti (Malta) mt_MT	Euro	EUR	€1,234,567.57 -€1,234,567.57
() my_MM	Myanmar Kyat	MMK	, , . K -, , . K
Nepali (Nepal) ne_NP	Nepalese Rupee	NPR	, , . - , , .
Nederlands (Aruba) nl_AW	Arubaanse gulden	AWG	Afl. 1.234.567,57 Afl. -1.234.567,57
Nederlands (België) nl_BE	Euro	EUR	€ 1.234.567,57 € -1.234.567,57
Nederlands (Nederland) nl_NL	Euro	EUR	€ 1.234.567,57 € -1.234.567,57
Nederlands (Suriname) nl_SR	Surinaamse dollar	SRD	\$ 1.234.567,57 \$ -1.234.567,57
Norsk (Norge) no_NO	Norsk krone	NOK	kr 1 234 567,57 kr -1 234 567,57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
() pa_IN	Indian Rupee	INR	12,34,567.57 - 12,34,567.57
Polski (Polska) pl_PL	Złoty polski	PLN	1 234 567,57 zł -1 234 567,57 zł
Pashto (Afghanistan) ps_AF	Afghanistan Afghani (New)	AFN	-
Português (Angola) pt_AO	Kwanza Angolano	AOA	1 234 567,57 Kz -1 234 567,57 Kz
Português (Brasil) pt_BR	Real brasileiro	BRL	R\$ 1.234.567,57 -R\$ 1.234.567,57
Português (Cabo Verde) pt_CV	Escudo de Cabo Verde	CVE	1 234 567\$57 -1 234 567\$57
Português (Moçambique) pt_MZ	Novo Metical Moçambicano	MZN	1 234 567,57 MTn -1 234 567,57 MTn
Português (Portugal) pt_PT	Euro	EUR	1 234 567,57 € -1 234 567,57 €
Português (São Tomé e Príncipe) pt_ST	Dobra de São Tomé e Príncipe	STN	1 234 567,57 Db -1 234 567,57 Db
Rumantsch (Svizra) rm_CH	Swiss Franc	CHF	1'234'567.57 CHF -1'234'567.57 CHF
Rundi (Burundi) rn_BI	Burundi Franc	BIF	1.234.567,57 FBu -1.234.567,57 FBu
Română (Republica Moldova) ro_MD	Leu moldovenesc	MDL	1.234.567,57 L -1.234.567,57 L
Română (România) ro_RO	Leu românesc	RON	1.234.567,57 RON -1.234.567,57 RON

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
Русский (Армения) ru_AM	Армянский драм	AMD	1 234 567,57 AMD -1 234 567,57 AMD
Русский (Беларусь) ru_BY	Белорусский рубль	BYN	1 234 567,57 Br -1 234 567,57 Br
Русский (Киргизия) ru_KG	Киргизский сом	KGS	1 234 567,57 сом -1 234 567,57 сом
Русский (Казахстан) ru_KZ	Казахстанский тенге	KZT	1 234 567,57 ₸ -1 234 567,57 ₸
Русский (Литва) ru_LT	Евро	EUR	1 234 567,57 € -1 234 567,57 €
Русский (Молдова) ru_MD	Молдавский лей	MDL	1 234 567,57 L -1 234 567,57 L
Русский (Польша) ru_PL	Польский злотый	PLN	1 234 567,57 PLN -1 234 567,57 PLN
Русский (Россия) ru_RU	Российский рубль	RUB	1 234 567,57 ₹ -1 234 567,57 ₹
Русский (Украина) ru_UA	Украинская гривна	UAH	1 234 567,57 ₴ -1 234 567,57 ₴
Serbian (Latin) (Bosnia and Herzegovina) sh_BA	Convertible Marks	BAM	1.234.567,57 KM -1.234.567,57 KM
Serbian (Latin) (Serbia) ¹ sh_CS	Serbian Dinar	CSD	1.234.567,57 CSD -1.234.567,57 CSD
Montenegrin (Montenegro) sh_ME	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Montenegrin (Montenegro, USD) sh_ME_USD	U.S. Dollar	USD	¤1,234,567.57 -¤1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
Slovenčina (Slovensko) sk_SK	Euro	EUR	1 234 567,57 € -1 234 567,57 €
Slovenščina (Slovenija) sl_SI	Evro	EUR	1.234.567,57 € -1.234.567,57 €
Samoaan (United States) sm_US	U.S. Dollar	USD	\$1,234,567.57 -\$1,234,567.57
Samoaan (Samoa) sm_WS	Samoa Tala	WST	WST 1,234,567.57 -WST 1,234,567.57
Somali (Djibouti) so_DJ	Djibouti Franc	DJF	Fdj 1,234,567.57 -Fdj 1,234,567.57
Somali (Somalia) so_SO	Somali Shilling	SOS	S 1,234,567.57 -S 1,234,567.57
Shqip (Shqipëri) sq_AL	Albanian Lek	ALL	1 234 567,57 Lekë -1 234 567,57 Lekë
Serbian (Cyrillic) (Bosnia and Herzegovina) sr_BA	Convertible Marks	BAM	1.234.567,57 KM -1.234.567,57 KM
Serbian (Cyrillic) (Serbia) ¹ sr_CS	Serbian Dinar	CSD	1.234.567,57 CSD -1.234.567,57 CSD
Српски (Србија) sr_RS	Serbian Dinar	RSD	1.234.567,57 RSD -1.234.567,57 RSD
Svenska (Sverige) sv_SE	Sverige Krona	SEK	1 234 567,57 kr -1 234 567,57 kr
Kiswahili (Kenya) sw_KE	Kenyan Shilling	KES	Ksh 1,234,567.57 -Ksh 1,234,567.57
() ta_IN	Indian Rupee	INR	12,34,567.57 - 12,34,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
() ta_LK	Sri Lanka Rupee	LKR	Rs. 12,34,567.57 -Rs. 12,34,567.57
() te_IN	Indian Rupee	INR	12,34,567.57 - 12,34,567.57
Tajik (Tajikistan) tg_TJ	Tajik Somoni	TJS	1 234 567,57 com. -1 234 567,57 com.
ไทย (ไทย) th_TH	บาท ไทย	THB	฿1,234,567.57 -฿1,234,567.57
Tigrinya (Ethiopia) ti_ET	Ethiopian Birr	ETB	Br 1,234,567.57 -Br 1,234,567.57
Tagalog (Pilipinas) tl_PH	Philippine Peso	PHP	1,234,567.57 - 1,234,567.57
Türkçe (Türkiye) tr_TR	Türk Lirası (Yeni)	TRY	1.234.567,57 - 1.234.567,57
Українська (Україна) uk_UA	Українська гривня	UAH	1 234 567,57 -1 234 567,57
()) ur_PK	Pakistani Rupee	PKR	Rs 1,234,567.57 -Rs 1,234,567.57
Uzbek (Latin, Uzbekistan) uz_LATN_UZ	Uzbekistan Sum	UZS	1 234 567,57 so m -1 234 567,57 so m
Ti ng Vi t (Vi t Nam) vi_VN	Đô ng Vi t Nam	VND	1.234.567,57 -1.234.567,57
IsiXhosa (eMzantsi Afrika) xh_ZA	South African Rand	ZAR	R 1 234 567.57 -R 1 234 567.57
Yoruba (Benin) yo_BJ	CFA Franc (BCEAO)	XOF	F CFA 1,234,567.57 -F CFA 1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
中文 (中国) zh_CN	人民币	CNY	¥1,234,567.57 -¥1,234,567.57
中文 (中国, CNH) zh_CN_CNH	人民币 (离岸)	CNH	CNH 1,234,567.57 -CNH 1,234,567.57
中文 (中国, 拼音顺序) zh_CN_PINYIN	人民币	CNY	¥1,234,567.57 -¥1,234,567.57
中文 (中国, 笔画顺序) zh_CN_STROKE	人民币	CNY	¥1,234,567.57 -¥1,234,567.57
zh_HK		HKD	HK\$1,234,567.57 -HK\$1,234,567.57
() zh_HK_STROKE		HKD	HK\$1,234,567.57 -HK\$1,234,567.57
zh_MO		MOP	MOP\$1,234,567.57 -MOP\$1,234,567.57
zh_MY		MYR	MYR 1,234,567.57 -MYR 1,234,567.57
zh_SG		SGD	\$1,234,567.57 -\$1,234,567.57
中文 (台湾) zh_TW	台幣	TWD	\$1,234,567.57 -\$1,234,567.57
中文 (台湾, 筆劃順序) zh_TW_STROKE	台幣	TWD	\$1,234,567.57 -\$1,234,567.57
IsiZulu (iNingizimu Afrika) zu_ZA	South African Rand	ZAR	R 1,234,567.57 -R 1,234,567.57

¹ The CSD currency is only available in single currency orgs and orgs that activated multiple currencies when CSD was the corporate currency. It represents the old Serbian Dinar used in Serbia and Montenegro from 2003 to 2006. Because it's no longer a valid ISO currency

code, it can be incompatible with other systems. If your org uses this currency, we recommend moving to the current Serbian Dinar currency, RSD. The corresponding locale is Serbian (Serbia) with the sr_RS locale code.

SEE ALSO:

[Set Your Personal or Organization-Wide Currency](#)

Salesforce Supported Locales and JDK Formats

Salesforce supported locales and their corresponding Oracle's Java Development Kit (JDK) formats for name, address, numbers, currencies, dates, and times. We use JDK version 11, which uses Common Locale Data Repository (CLDR) version 33. We replace these formats with the International Components for Unicode (ICU) formats in Spring '24. Or, now you can adopt the new formats through the Enable ICU Formats release update.

[Supported Number, Name, and Address Formats \(JDK\)](#)

Salesforce supported locales with their Oracle Java Development Kit (JDK) formats for numbers, name, and address.

[Supported Date and Time Formats \(JDK\)](#)

The start day of the week and Oracle's Java Development Kit (JDK) date and time formats for each Salesforce supported locale.

[Supported Currencies \(JDK\)](#)

Salesforce supported currencies, listed by locale with Oracle's Java Development Kit (JDK) formats.

SEE ALSO:

[Adopt the ICU Locale Formats](#)

Supported Number, Name, and Address Formats (JDK)

Salesforce supported locales with their Oracle Java Development Kit (JDK) formats for numbers, name, and address.



Note: Review these important details about the data in this table.

- We recommend viewing this information in Salesforce Help. Not all characters appear correctly in PDFs.
- Arabic-Indic is the numeral system for certain locales and languages. If you want to use the Hindu-Arabic numeral system for those languages and locales, contact Salesforce Customer Support.

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
Afrikaans (Suid-Afrika)	1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode
af_ZA	-1 234 567,567		

EDITIONS

Available in: Lightning Experience and Salesforce Classic ([not available in all orgs](#))

Available in: **Group, Professional, Enterprise, Performance, Unlimited, Database.com,** and **Developer** Editions

EDITIONS

Available in: Lightning Experience and Salesforce Classic ([not available in all orgs](#))

Available in: **Group, Professional, Enterprise, Performance, Unlimited, Database.com,** and **Developer** Editions

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
() am_ET	1,234,567.567 -1,234,567.567	Ms. FName LName	State Country Address Line 1, Address Line 2 ZipCode City State Country
)) ar_AE	-	Ms. FName LName	Address Line 1, Address Line 2 State ZipCode City Country
)) ar_BH	-	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
)) ar_DZ	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
)) ar_EG	-	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
)) ar_IQ	-	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
)) ar_JO	-	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
)) ar_KW	-	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
)) ar_LB	-	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
)) ar_LY	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
)) ar_MA	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
)) ar_OM	-	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
)) ar_QA	-	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
)) ar_SA	-	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
)) ar_SD	-	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
)) ar_SY	-	Ms. FName LName	Country Address Line 1, Address Line 2 City, State ZipCode Country
)) ar_TN	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
)) ar_YE	-	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Azerbaijani (Azerbaijan) az_AZ	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Belarusian (Belarus) be_BY	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Български (България) bg_BG	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
() bn_BD	, , , . - , , , .	Ms. FName LName	Address Line 1, Address Line 2 City - ZipCode State Country
() bn_IN	, , , . - , , , .	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			State Country
Bosanski (Bosna i Hercegovina) bs_BA	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Català (Espanya) ca_ES	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Čeština (Česko) cs_CZ	1 234 567,57 -1 234 567,57	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Cymraeg (Y Deyrnas Unedig) cy_GB	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
Dansk (Danmark) da_DK	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Deutsch (Österreich) de_AT	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Deutsch (Belgien) de_BE	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
Deutsch (Schweiz) de_CH	1'234'567.567 -1'234'567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Deutsch (Deutschland) de_DE	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Deutsch (Luxemburg) de_LU	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Dzongkha (Bhutan) dz_BT	, , . - , , .	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Ελληνικά (Κύπρος) el_CY	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Ελληνικά (Ελλάδα) el_GR	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
English (United Arab Emirates) en_AE	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 State ZipCode City Country
English (Antigua & Barbuda) en_AG	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
English (Australia) en_AU	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
English (Barbados) en_BB	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Belgium) en_BE	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Bermuda) en_BM	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Bahamas) en_BS	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Botswana) en_BW	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Belize) en_BZ	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Canada) en_CA	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
English (Cameroon) en_CM	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Cyprus) en_CY	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
English (Germany) en_DE	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
English (Eritrea) en_ER	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Fiji) en_FJ	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Falkland Islands) en_FK	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (United Kingdom) en_GB	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
English (Ghana) en_GH	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Gibraltar) en_GI	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Gambia) en_GM	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Guyana) en_GY	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Hong Kong SAR China) en_HK	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Indonesia) en_ID	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
English (Ireland) en_IE	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
English (Israel) en_IL	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			ZipCode City State Country
English (India) en_IN	12,34,567.567 -12,34,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Italy) en_IT	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
English (Jamaica) en_JM	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
English (Kenya) en_KE	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Cayman Islands) en_KY	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 State ZipCode City Country
English (Liberia) en_LR	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
English (Madagascar) en_MG	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			State Country
English (Malta) en_MT	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Mauritius) en_MU	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
English (Malawi) en_MW	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Malaysia) en_MY	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
English (Namibia) en_NA	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Nigeria) en_NG	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Netherlands) en_NL	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
English (New Zealand) en_NZ	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Papua New Guinea) en_PG	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Philippines) en_PH	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2, City ZipCode State Country
English (Pakistan) en_PK	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City-ZipCode State Country
English (Rwanda) en_RW	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Solomon Islands) en_SB	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Seychelles) en_SC	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
English (Singapore) en_SG	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			State Country
English (St. Helena) en_SH	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Sierra Leone) en_SL	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Sierra Leone, SLL) en_SL_SLL	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Sint Maarten) en_SX	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Eswatini) en_SZ	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
English (Tonga) en_TO	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Trinidad & Tobago) en_TT	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
English (Tanzania) en_TZ	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
English (Uganda) en_UG	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (United States) en_US	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Vanuatu) en_VU	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Samoa) en_WS	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (South Africa) en_ZA	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Español (Argentina) es_AR	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Español (Bolivia) es_BO	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			City, State ZipCode Country
Español (Chile) es_CL	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Español (Colombia) es_CO	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State, ZipCode Country
Español (Costa Rica) es_CR	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 State, City ZipCode Country
Español (Cuba) es_CU	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Español (República Dominicana) es_DO	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Español (Ecuador) es_EC	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Español (España) es_ES	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			Country
Español (Guatemala) es_GT	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode-City State Country
Español (Honduras) es_HN	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Español (México) es_MX	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City, State Country
Español (Nicaragua) es_NI	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City, State Country
Español (Panamá) es_PA	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
Español (Perú) es_PE	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Español (Puerto Rico) es_PR	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			State Country
Español (Paraguay) es_PY	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Español (El Salvador) es_SV	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode-City State Country
Español (Estados Unidos) es_US	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Español (Uruguay) es_UY	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Español (Venezuela) es_VE	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode, State Country
Eesti (Eesti) et_EE	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Euskara (Espainia) eu_ES	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
)) fa_IR	—	Ms. FName LName	State City

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			Address Line 1, Address Line 2 ZipCode Country
Suomi (Suomi) fi_FI	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Français (Belgique) fr_BE	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Français (Canada) fr_CA	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
Français (Suisse) fr_CH	1'234'567.567 -1'234'567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Français (France) fr_FR	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Français (Guinée) fr_GN	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Français (Haïti) fr_HT	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
Français (Comores) fr_KM	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Français (Luxembourg) fr_LU	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Français (Maroc) fr_MA	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Français (Monaco) fr_MC	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Français (Mauritanie) fr_MR	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Français (Wallis-et-Futuna) fr_WF	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Gaeilge (Éire) ga_IE	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
() gu_IN	12,34,567.567 -12,34,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			State Country
Ōlelo Hawai i (Amelika Hui Pū la) haw_US	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
() hi_IN	12,34,567.567 -12,34,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Hmong (United States) hmn_US	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Hrvatski (Hrvatska) hr_HR	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Hrvatski (Hrvatska, HRK) hr_HR_HRK	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Haitian Creole (Haiti) ht_HT	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Haitian Creole (United States) ht_US	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
Magyar (Magyarország) hu_HU	1 234 567,567 -1 234 567,567	LName FName	City Address Line 1, Address Line 2 ZipCode State Country
() hy_AM	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Indonesia (Indonesia) in_ID	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
Íslenska (Ísland) is_IS	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Italiano (Svizzera) it_CH	1'234'567.567 -1'234'567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Italiano (Italia) it_IT	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
)) iw_IL	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
日本語 (日本) ja_JP	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City State ZipCode Country
Yiddish (United States) ji_US	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
() ka_GE	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
аза тілі (аза стан) kk_KZ	1 234 567,567 -1 234 567,567	Ms. FName LName	ZipCode State City Address Line 1, Address Line 2 Country
Kalaallisut (Kalaallit Nunaat) kl_GL	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
() km_KH	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
() kn_IN	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
한국어 (북한) ko_KP	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
한국어 (대한민국) ko_KR	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
Kyrgyz (Kyrgyzstan) ky_KG	1 234 567,567 -1 234 567,567	Ms. FName LName	ZipCode City Address Line 1, Address Line 2 State Country
Lëtzebuergesch (Lëtzebuerg) lb_LU	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Lao (Laos) lo_LA	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Lietuvių (Lietuva) lt_LT	1 234 567,57 -1 234 567,57	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Luba-Katanga (Congo - Kinshasa) lu_CD	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Latviešu (Latvija) lv_LV	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, ZipCode

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			State Country
Te reo (New Zealand) mi_NZ	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Македонски (Северна Македонија) mk_MK	1.234.567,567 (1.234.567,567)	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
() ml_IN	12,34,567.567 -12,34,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
() mr_IN	, , , . - , , , .	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Melayu (Brunei) ms_BN	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Melayu (Malaysia) ms_MY	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Malti (Malta) mt_MT	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
() my_MM	, , . - , , .	Ms. FName LName	Address Line 1, Address Line 2 City, ZipCode State Country
Nepali (Nepal) ne_NP	, , . - , , .	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Nederlands (Aruba) nl_AW	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Nederlands (België) nl_BE	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Nederlands (Nederland) nl_NL	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Nederlands (Suriname) nl_SR	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
Norsk (Norge) no_NO	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
() pa_IN	12,34,567.567 -12,34,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			State Country
Polski (Polska) pl_PL	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Pashto (Afghanistan) ps_AF	-	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Português (Angola) pt_AO	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Português (Brasil) pt_BR	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City-State ZipCode Country
Português (Cabo Verde) pt_CV	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Português (Moçambique) pt_MZ	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Português (Portugal) pt_PT	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			State Country
Português (São Tomé e Príncipe) pt_ST	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Rumantsch (Svizra) rm_CH	1'234'567.567 -1'234'567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Rundi (Burundi) rn_BI	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Română (Republica Moldova) ro_MD	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Română (România) ro_RO	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Русский (Армения) ru_AM	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Русский (Беларусь) ru_BY	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
Русский (Киргизия) ru_KG	1 234 567,567 -1 234 567,567	Ms. FName LName	ZipCode City Address Line 1, Address Line 2 State Country
Русский (Казахстан) ru_KZ	1 234 567,567 -1 234 567,567	Ms. FName LName	ZipCode State City Address Line 1, Address Line 2 Country
Русский (Литва) ru_LT	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Русский (Молдова) ru_MD	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Русский (Польша) ru_PL	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Русский (Россия) ru_RU	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
Русский (Украина) ru_UA	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City State

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			ZipCode Country
Serbian (Latin) (Bosnia and Herzegovina) sh_BA	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Serbian (Latin) (Serbia) sh_CS	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Montenegrin (Montenegro) sh_ME	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Montenegrin (Montenegro, USD) sh_ME_USD	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Slovenčina (Slovensko) sk_SK	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Slovenščina (Slovenija) sl_SI	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Samoan (United States) sm_US	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Samoan (Samoa) sm_WS	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
			City, State ZipCode Country
Somali (Djibouti) so_DJ	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Somali (Somalia) so_SO	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Shqip (Shqipëri) sq_AL	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Serbian (Cyrillic) (Bosnia and Herzegovina) sr_BA	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Serbian (Cyrillic) (Serbia) sr_CS	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Српски (Србија) sr_RS	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Svenska (Sverige) sv_SE	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
Kiswahili (Kenya) sw_KE	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
() ta_IN	12,34,567.567 -12,34,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
() ta_LK	12,34,567.567 -12,34,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
() te_IN	12,34,567.567 -12,34,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country
Tajik (Tajikistan) tg_TJ	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
ไทย (ไทย) th_TH	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
Tigrinya (Ethiopia) ti_ET	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
Tagalog (Pilipinas) tl_PH	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2, City ZipCode State Country
Türkçe (Türkiye) tr_TR	1.234.567,567 -1.234.567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City/State Country
Українська (Україна) uk_UA	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 City State ZipCode Country
Urdu (Urdu) ur_PK	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City-ZipCode State Country
Uzbek (Latin, Uzbekistan) uz_LATN_UZ	1 234 567,567 -1 234 567,567	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Tiếng Việt (Việt Nam) vi_VN	1.234.567,567 -1.234.567,567	LName FName	Address Line 1, Address Line 2 City State ZipCode Country
IsiXhosa (eMzantsi Afrika) xh_ZA	1 234 567.567 -1 234 567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
Yoruba (Benin) yo_BJ	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
中文 (中国) zh_CN	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
中文 (中国, CNH) zh_CN_CNH	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
中文 (中国, 拼音顺序) zh_CN_PINYIN	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
中文 (中国, 笔画顺序) zh_CN_STROKE	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
zh_HK	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
() zh_HK_STROKE	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
zh_MO	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country

LOCALE NAME AND CODE	NUMBER FORMAT	NAME FORMAT	ADDRESS FORMAT
zh_MY	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 ZipCode City State Country
zh_SG	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City ZipCode State Country
中文 (台灣) zh_TW	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
中文 (台灣, 筆劃順序) zh_TW_STROKE	1,234,567.567 -1,234,567.567	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
IsiZulu (iNingizimu Afrika) zu_ZA	1,234,567.567 -1,234,567.567	Ms. FName LName	Address Line 1, Address Line 2 City ZipCode State Country

Supported Date and Time Formats (JDK)

The start day of the week and Oracle’s Java Development Kit (JDK) date and time formats for each Salesforce supported locale.

We use three variations of date and time formats across the Salesforce application: short, medium, and long. All three formats are listed for each locale by length, with the short format listed first. For unauthenticated guest users, date and time formats on Salesforce Sites are based on the user’s browser settings instead of the user’s personal locale.

 **Note:** The user’s `Language` setting determines the language of the AM/PM designator in date/time fields. For example, if the user’s language is English, times in the Chinese (Singapore) locale display with English AM/PM designators.

 **Note:** We recommend viewing this information in Salesforce Help. Not all characters appear correctly in PDFs.

EDITIONS

Available in: Lightning Experience and Salesforce Classic ([not available in all orgs](#))

Available in: **Group, Professional, Enterprise, Performance, Unlimited, Database.com,** and **Developer** Editions

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
Afrikaans (Suid-Afrika) af_ZA	2008-01-28 16:30 28 Jan. 2008 16:30:05 2008-01-28 16:30:05 GMT-8	16:30	Sunday – Saturday
() am_ET	28/01/2008 4:30 28 2008 4:30:05 28/01/2008 4:30:05 -8	4:30	Sunday – Saturday
)) ar_AE	// ,: / / , : : // , : : -	:	Saturday – Sunday
)) ar_BH	// ,: / / , : : // , : : -	:	Saturday – Sunday
)) ar_DZ	28 /1 /2008, 4:30 28 /01 /2008, 4:30:05 28 /1 /2008, 4:30:05 -8	4:30	Saturday – Sunday
)) ar_EG	// ,: / / , : : // , : : -	:	Saturday – Sunday
)) ar_IQ	// ,: / / , : :	:	Saturday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	// ,:: -		
)) ar_JO	// : // :: // - ::	:	Saturday – Sunday
)) ar_KW	// ,: // ,:: // ,:: -	:	Saturday – Sunday
)) ar_LB	// : // :: // - ::	:	Monday – Sunday
)) ar_LY	28 /1 /2008, 4:30 28 /01 /2008, 4:30:05 28 /1 /2008, 4:30:05 -8	4:30	Saturday – Sunday
)) ar_MA	28 /1 /2008, 16:30 28 /01 /2008, 16:30:05 28 /1 /2008, 16:30:05 -8	16:30	Monday – Sunday
)) ar_OM	// ,: // ,:: // ,:: -	:	Saturday – Sunday
)) ar_QA	// ,: // ,:: // ,:: -	:	Saturday – Sunday
)) ar_SA	// : // :: // - ::	:	Sunday – Saturday
)) ar_SD	// ,: // ,:: // ,:: -	:	Saturday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
)) ar_SY	// : // :: // - ::	:	Saturday – Sunday
)) ar_TN	28/1/2008, 4:30 28/01/2008, 4:30:05 28/1/2008, 4:30:05 -8	4:30	Monday – Sunday
)) ar_YE	// , : // , : : // , : : -	:	Sunday – Saturday
Azerbaijani (Azerbaijan) az_AZ	28.01.2008 16:30 28 Jan 2008 16:30:05 28.01.2008 16:30:05 GMT-8	16:30	Monday – Sunday
Belarusian (Belarus) be_BY	28.1.2008 16.30 28.1.2008 16.30.05 28.1.2008 16.30.05 PST	16.30	Monday – Sunday
Български (България) bg_BG	28.01.2008 16:30 28.01.2008 16:30:05 28.01.2008 16:30:05 Гринуич-8	16:30	Monday – Sunday
() bn_BD	// : PM , : : PM // : : PM GMT -	: PM	Sunday – Saturday
() bn_IN	// : PM , : : PM // : : PM GMT -	: PM	Sunday – Saturday
Bosanski (Bosna i Hercegovina) bs_BA	28. 1. 2008. 16:30 28. jan 2008. 16:30:05 28. 1. 2008. 16:30:05 GMT -8	16:30	Monday – Sunday
Català (Espanya) ca_ES	28/01/2008 16:30 28/01/2008 16:30:05	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28/01/2008 16:30:05 PST		
Čeština (Česko) cs_CZ	28.1.2008 16:30 28.1.2008 16:30:05 28.1.2008 16:30:05 PST	16:30	Monday – Sunday
Cymraeg (Y Deyrnas Unedig) cy_GB	28/01/2008 16:30 28 Ion 2008 16:30:05 28/01/2008 16:30:05 GMT-8	16:30	Monday – Sunday
Dansk (Danmark) da_DK	28-01-2008 16:30 28-01-2008 16:30:05 28-01-2008 16:30:05 PST	16:30	Monday – Sunday
Deutsch (Österreich) de_AT	28.01.2008 16:30 28.01.2008 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
Deutsch (Belgien) de_BE	28.01.2008, 16:30 28.01.2008, 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Deutsch (Schweiz) de_CH	28.01.2008 16:30 28.01.2008 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
Deutsch (Deutschland) de_DE	28.01.2008 16:30 28.01.2008 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
Deutsch (Luxemburg) de_LU	28.01.2008 16:30 28.01.2008 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
Dzongkha (Bhutan) dz_BT	- - PM Jan : : PM - - : PM -	PM	Sunday – Saturday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
Ελληνικά (Κύπρος) el_CY	28/01/2008 4:30 MM 28 Ιαν 2008 4:30:05 MM 28/01/2008 4:30:05 MM PST	4:30 MM	Monday – Sunday
Ελληνικά (Ελλάδα) el_GR	28/1/2008 4:30 μμ 28 Ιαν 2008 4:30:05 μμ 28/1/2008 4:30:05 μμ PST	4:30 μμ	Monday – Sunday
English (United Arab Emirates) en_AE	28/01/2008, 4:30 PM 28 Jan 2008, 4:30:05 PM 28/01/2008, 4:30:05 PM GMT-8	4:30 PM	Saturday – Sunday
English (Antigua & Barbuda) en_AG	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (Australia) en_AU	28/01/2008 4:30 PM 28/01/2008 4:30:05 PM 28/01/2008 4:30:05 PM	4:30 PM	Monday – Sunday
English (Barbados) en_BB	28/01/2008 16:30 28/01/2008 16:30:05 28/01/2008 16:30:05 PST	4:30 pm	Monday – Sunday
English (Belgium) en_BE	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Bermuda) en_BM	28/01/2008 16:30 28/01/2008 16:30:05 28/01/2008 16:30:05 PST	4:30 pm	Monday – Sunday
English (Bahamas) en_BS	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (Botswana) en_BW	28/01/2008, 16:30 28 Jan 2008, 16:30:05	16:30	Sunday – Saturday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28/01/2008, 16:30:05 GMT-8		
English (Belize) en_BZ	28/01/2008, 16:30 28-Jan-2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
English (Canada) en_CA	28/01/2008 4:30 PM 28-Jan-2008 4:30:05 PM 28/01/2008 4:30:05 PST PM	4:30 PM	Sunday – Saturday
English (Cameroon) en_CM	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Cyprus) en_CY	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Germany) en_DE	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Eritrea) en_ER	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Fiji) en_FJ	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Falkland Islands) en_FK	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (United Kingdom) en_GB	28/01/2008 16:30 28-Jan-2008 16:30:05 28/01/2008 16:30:05 PST	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
English (Ghana) en_GH	28/01/2008 16:30 28/01/2008 16:30:05 28/01/2008 16:30:05 PST	4:30 pm	Monday – Sunday
English (Gibraltar) en_GI	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Gambia) en_GM	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Guyana) en_GY	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Hong Kong SAR China) en_HK	28/1/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/1/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (Indonesia) en_ID	28/01/2008 16:30 28/01/2008 16:30:05 28/01/2008 16:30:05 PST	4:30 PM	Sunday – Saturday
English (Ireland) en_IE	28/01/2008 16:30 28-Jan-2008 16:30:05 28/01/2008 16:30:05 PST	16:30	Monday – Sunday
English (Israel) en_IL	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
English (India) en_IN	28/1/2008 4:30 pm 28 Jan, 2008 4:30:05 pm 28/1/2008 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (Italy) en_IT	1/28/2008 4:30 PM Jan 28, 2008 4:30:05 PM	4:30 PM	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	1/28/2008 4:30:05 PM PST		
English (Jamaica) en_JM	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (Kenya) en_KE	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
English (Cayman Islands) en_KY	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Liberia) en_LR	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Madagascar) en_MG	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Malta) en_MT	28/01/2008 16:30 28 Jan 2008 16:30:05 28/01/2008 16:30:05 PST	16:30	Sunday – Saturday
English (Mauritius) en_MU	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Malawi) en_MW	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Malaysia) en_MY	28/01/2008 16:30 28/01/2008 16:30:05 28/01/2008 16:30:05 PST	4:30 pm	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
English (Namibia) en_NA	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Nigeria) en_NG	28/01/2008 16:30 28/01/2008 16:30:05 28/01/2008 16:30:05 PST	16:30	Monday – Sunday
English (Netherlands) en_NL	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (New Zealand) en_NZ	28/01/2008 4:30 PM 28/01/2008 4:30:05 PM 28/01/2008 4:30:05 PM	4:30 PM	Monday – Sunday
English (Papua New Guinea) en_PG	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Philippines) en_PH	1/28/2008 4:30 PM 01 28, 2008 4:30:05 PM 1/28/2008 4:30:05 PM PST	4:30 PM	Sunday – Saturday
English (Pakistan) en_PK	28/01/2008, 4:30 pm 28-Jan-2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (Rwanda) en_RW	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Solomon Islands) en_SB	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Seychelles) en_SC	28/01/2008, 16:30 28 Jan 2008, 16:30:05	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28/01/2008, 16:30:05 GMT-8		
English (Singapore) en_SG	28/01/2008 16:30 28/01/2008 16:30:05 28/01/2008 16:30:05 PST	4:30 PM	Sunday – Saturday
English (St. Helena) en_SH	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Sierra Leone) en_SL	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Sierra Leone, SLL) en_SL_SLL	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Sint Maarten) en_SX	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (Eswatini) en_SZ	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Tonga) en_TO	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Trinidad & Tobago) en_TT	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (Tanzania) en_TZ	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
English (Uganda) en_UG	28/01/2008, 16:30 28 Jan 2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
English (United States) en_US	1/28/2008 4:30 PM Jan 28, 2008 4:30:05 PM 1/28/2008 4:30:05 PM PST	4:30 PM	Sunday – Saturday
English (Vanuatu) en_VU	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Monday – Sunday
English (Samoa) en_WS	28/01/2008, 4:30 pm 28 Jan 2008, 4:30:05 pm 28/01/2008, 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
English (South Africa) en_ZA	2008/01/28 4:30 PM 28 Jan 2008 4:30:05 PM 2008/01/28 4:30:05 PM	4:30 PM	Sunday – Saturday
Español (Argentina) es_AR	28/01/2008 16:30 28/01/2008 16:30:05 28/01/2008 16:30:05 PST	16:30	Monday – Sunday
Español (Bolivia) es_BO	28-01-2008 04:30 PM 28-01-2008 04:30:05 PM 28-01-2008 04:30:05 PM PST	04:30 PM	Monday – Sunday
Español (Chile) es_CL	28-01-2008 16:30 28-01-2008 16:30:05 28-01-2008 16:30:05 PST	16:30	Monday – Sunday
Español (Colombia) es_CO	28/01/2008 04:30 PM 28/01/2008 04:30:05 PM 28/01/2008 04:30:05 PM PST	04:30 PM	Sunday – Saturday
Español (Costa Rica) es_CR	28/01/2008 04:30 PM 28/01/2008 04:30:05 PM	04:30 PM	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28/01/2008 04:30:05 PM PST		
Español (Cuba) es_CU	28/1/2008, 16:30 28 ene 2008 16:30:05 28/1/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Español (República Dominicana) es_DO	28/01/2008 04:30 PM 28/01/2008 04:30:05 PM 28/01/2008 04:30:05 PM PST	04:30 PM	Sunday – Saturday
Español (Ecuador) es_EC	28/01/2008 16:30 28/01/2008 16:30:05 28/01/2008 16:30:05 PST	16:30	Monday – Sunday
Español (España) es_ES	28/01/2008 16:30 28-ene-2008 16:30:05 28/01/2008 16:30:05 PST	16:30	Monday – Sunday
Español (Guatemala) es_GT	28/01/2008 04:30 PM 28/01/2008 04:30:05 PM 28/01/2008 04:30:05 PM PST	04:30 PM	Sunday – Saturday
Español (Honduras) es_HN	01-28-2008 04:30 PM 01-28-2008 04:30:05 PM 01-28-2008 04:30:05 PM PST	04:30 PM	Sunday – Saturday
Español (México) es_MX	28/01/2008 04:30 PM 28/01/2008 04:30:05 PM 28/01/2008 04:30:05 PM PST	04:30 PM	Sunday – Saturday
Español (Nicaragua) es_NI	01-28-2008 04:30 PM 01-28-2008 04:30:05 PM 01-28-2008 04:30:05 PM PST	04:30 PM	Sunday – Saturday
Español (Panamá) es_PA	01/28/2008 04:30 PM 01/28/2008 04:30:05 PM 01/28/2008 04:30:05 PM PST	04:30 PM	Sunday – Saturday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
Español (Perú) es_PE	28/01/2008 04:30 p. m. 28/01/2008 04:30:05 p. m. 28/01/2008 04:30:05 p. m. GMT-8	04:30 p. m.	Sunday – Saturday
Español (Puerto Rico) es_PR	01-28-2008 04:30 PM 01-28-2008 04:30:05 PM 01-28-2008 04:30:05 PM PST	04:30 PM	Sunday – Saturday
Español (Paraguay) es_PY	28/01/2008 04:30 PM 28/01/2008 04:30:05 PM 28/01/2008 04:30:05 PM PST	04:30 PM	Sunday – Saturday
Español (El Salvador) es_SV	01-28-2008 04:30 PM 01-28-2008 04:30:05 PM 01-28-2008 04:30:05 PM PST	04:30 PM	Sunday – Saturday
Español (Estados Unidos) es_US	1/28/2008 4:30 p.m. ene 28, 2008 4:30:05 p.m. 1/28/2008 4:30:05 p.m. PST	4:30 p.m.	Sunday – Saturday
Español (Uruguay) es_UY	28/01/2008 04:30 PM 28/01/2008 04:30:05 PM 28/01/2008 04:30:05 PM PST	04:30 PM	Monday – Sunday
Español (Venezuela) es_VE	28/01/2008 04:30 PM 28/01/2008 04:30:05 PM 28/01/2008 04:30:05 PM PST	04:30 PM	Sunday – Saturday
Eesti (Eesti) et_EE	28.01.2008 16:30 28.01.2008 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
Euskara (Espainia) eu_ES	2008/1/28 16:30 2008(e)ko urt. 28(a) 16:30:05 2008/1/28 16:30:05 (PST)	16:30	Monday – Sunday
)) fa_IR	: // ::	:	Saturday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	:: // (-)		
Suomi (Suomi) fi_FI	28.1.2008 16:30 28.1.2008 16:30:05 28.1.2008 klo 16.30.05	16:30	Monday – Sunday
Français (Belgique) fr_BE	28/01/2008 16:30 28-janv.-2008 16:30:05 28/01/2008 16:30:05 PST	16:30	Monday – Sunday
Français (Canada) fr_CA	2008-01-28 16:30 2008-01-28 16:30:05 2008-01-28 16:30:05 HNP	16:30	Sunday – Saturday
Français (Suisse) fr_CH	28.01.2008 16:30 28 janv. 2008 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
Français (France) fr_FR	28/01/2008 16:30 28 janv. 2008 16:30:05 28/01/2008 16:30:05 PST	16:30	Monday – Sunday
Français (Guinée) fr_GN	28/01/2008 16:30 28 janv. 2008, 16:30:05 28/01/2008 16:30:05 UTC–8	16:30	Monday – Sunday
Français (Haïti) fr_HT	28/01/2008 16:30 28 janv. 2008, 16:30:05 28/01/2008 16:30:05 UTC–8	16:30	Monday – Sunday
Français (Comores) fr_KM	28/01/2008 16:30 28 janv. 2008, 16:30:05 28/01/2008 16:30:05 UTC–8	16:30	Monday – Sunday
Français (Luxembourg) fr_LU	28/01/2008 16:30 28 janv. 2008, 16:30:05 28/01/2008 16:30:05 UTC–8	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
Français (Maroc) fr_MA	28/01/2008 16:30 28 jan. 2008, 16:30:05 28/01/2008 16:30:05 UTC-8	16:30	Monday – Sunday
Français (Monaco) fr_MC	28/01/2008 16:30 28 janv. 2008, 16:30:05 28/01/2008 16:30:05 UTC-8	16:30	Monday – Sunday
Français (Mauritanie) fr_MR	28/01/2008 4:30 PM 28 janv. 2008, 4:30:05 PM 28/01/2008 4:30:05 PM UTC-8	4:30 PM	Monday – Sunday
Français (Wallis-et-Futuna) fr_WF	28/01/2008 16:30 28 janv. 2008, 16:30:05 28/01/2008 16:30:05 UTC-8	16:30	Monday – Sunday
Gaeilge (Éire) ga_IE	28/01/2008 16:30 28 Ean 2008 16:30:05 28/01/2008 16:30:05 ACAC	16:30	Monday – Sunday
() gu_IN	28/1/2008 04:30 PM 28 , 2008 04:30:05 PM 28/1/2008 04:30:05 PM GMT-8	04:30 PM	Sunday – Saturday
Ōlelo Hawai i (Amelika Hui Pū la) haw_US	28/i/2008 4:30 PM 28 lan. 2008 4:30:05 PM 28/i/2008 4:30:05 PM GMT-8	4:30 PM	Sunday – Saturday
() hi_IN	28/1/2008 4:30 pm 28 , 2008 4:30:05 pm 28/1/2008 4:30:05 pm GMT-8	4:30 pm	Sunday – Saturday
Hmong (United States) hmn_US	1/28/2008 4:30 PM Jan 28, 2008 4:30:05 PM 1/28/2008 4:30:05 PM PST	4:30 PM	Sunday – Saturday
Hrvatski (Hrvatska) hr_HR	28.01.2008. 16:30 28.01.2008. 16:30:05	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28.01.2008. 16:30:05 PST		
Hrvatski (Hrvatska, HRK) hr_HR_HRK	28.01.2008. 16:30 28.01.2008. 16:30:05 28.01.2008. 16:30:05 PST	16:30	Monday – Sunday
Haitian Creole (Haiti) ht_HT	1/28/2008 4:30 PM Jan 28, 2008 4:30:05 PM 1/28/2008 4:30:05 PM PST	4:30 PM	Monday – Sunday
Haitian Creole (United States) ht_US	1/28/2008 4:30 PM Jan 28, 2008 4:30:05 PM 1/28/2008 4:30:05 PM PST	4:30 PM	Sunday – Saturday
Magyar (Magyarország) hu_HU	2008.01.28. 16:30 2008.01.28. 16:30:05 2008.01.28. 16:30:05 PST	16:30	Monday – Sunday
() hy_AM	28.01.2008, 16:30 28 , 2008 ., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Indonesia (Indonesia) in_ID	28/01/2008 16:30 28 Jan 2008 16:30:05 28/01/2008 16:30:05	16:30	Sunday – Saturday
Íslenska (Ísland) is_IS	28.1.2008 16:30 28.1.2008 16:30:05 28.1.2008 16:30:05 PST	16:30	Monday – Sunday
Italiano (Svizzera) it_CH	28.01.2008 16:30 28-gen-2008 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
Italiano (Italia) it_IT	28/01/2008 16.30 28-gen-2008 16.30.05 28/01/2008 16.30.05 PST	16.30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
)) iw_IL	16:30 28/01/2008 16:30:05 28/01/2008 16:30:05 PST 28/01/2008	16:30	Sunday – Saturday
日本語 (日本) ja_JP	2008/01/28 16:30 2008/01/28 16:30:05 2008/01/28 16:30:05 PST	16:30	Sunday – Saturday
Yiddish (United States) ji_US	1/28/2008, 4:30 PM Jan 28, 2008, 4:30:05 PM 1/28/2008, 4:30:05 PM PST	4:30 PM	Sunday – Saturday
() ka_GE	28.01.2008, 16:30 28 . 2008, 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
аза тілі (аза стан) kk_KZ	28.01.2008, 16:30 2008 ж. 28 а., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Kalaallisut (Kalaallit Nunaat) kl_GL	2008-01-28 16.30 2008 jan 28 16.30.05 2008-01-28 16.30.05 GMT-8	16.30	Monday – Sunday
() km_KH	28/1/2008, 4:30 PM 28 2008, 4:30:05 PM 28/1/2008, 4:30:05 PM -8	4:30 PM	Sunday – Saturday
() kn_IN	28/1/2008 04:30 28, 2008 04:30:05 28/1/2008 04:30:05 GMT-8	04:30	Sunday – Saturday
한국어 (북한) ko_KP	2008. 1. 28. 오후 4:30 2008. 1. 28. 오후 4:30:05 2008. 1. 28. 오후 4:30:05 GMT-8	오후 4:30	Monday – Sunday
한국어 (대한민국)	2008. 1. 28 오후 4:30	오후 4:30	Sunday – Saturday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
ko_KR	2008. 1. 28 오후 4:30:05 2008. 1. 28 오후 4시 30분 05초		
Kyrgyz (Kyrgyzstan) ky_KG	28/1/2008 16:30 2008-ж., 28-Jan 16:30:05 28/1/2008 16:30:05 GMT-8	16:30	Monday – Sunday
Lëtzebuergesch (Lëtzebuerg) lb_LU	28.01.2008 16:30 28. Jan. 2008 16:30:05 28.01.2008 16:30:05 GMT-8	16:30	Monday – Sunday
Lao (Laos) lo_LA	28/1/2008, 16:30 28 Jan 2008, 16:30:05 28/1/2008, 16 30 05 GMT-8	16:30	Sunday – Saturday
Lietuvių (Lietuva) lt_LT	2008.1.28 16:30 2008-01-28 16:30:05 2008.1.28 16:30:05 PST	16:30	Monday – Sunday
Luba-Katanga (Congo - Kinshasa) lu_CD	28/1/2008 16:30 28 Jan 2008 16:30:05 28/1/2008 16:30:05 GMT-8	16:30	Monday – Sunday
Latviešu (Latvija) lv_LV	28.01.2008 16:30 28.01.2008 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
Te reo (New Zealand) mi_NZ	28-01-2008 4:30 PM 28 Kohi 2008 4:30:05 PM 28-01-2008 4:30:05 PM GMT-8	4:30 PM	Monday – Sunday
Македонски (Северна Македонија) mk_MK	28.1.2008 16:30 28.1.2008 16:30: 28.1.2008 16:30:05 PST	16:30	Monday – Sunday
() ml_IN	28/1/2008 4:30 PM 2008, 28 4:30:05 PM	4:30 PM	Sunday – Saturday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28/1/2008 4:30:05 PM -8		
() mr_IN	// , : PM , , : : PM // , : : PM [GMT]-	: PM	Sunday – Saturday
Melayu (Brunei) ms_BN	28/01/2008, 4:30 PTG 28 Jan 2008, 4:30:05 PTG 28/01/2008, 4:30:05 PTG GMT-8	4:30 PTG	Monday – Sunday
Melayu (Malaysia) ms_MY	28/01/2008 4:30 PM 28 Januari 2008 4:30:05 PM 28/01/2008 4:30:05 PM PST	4:30 PM	Monday – Sunday
Malti (Malta) mt_MT	28/01/2008 16:30 28 Jan 2008 16:30:05 28/01/2008 16:30:05 PST	16:30	Sunday – Saturday
() my_MM	- - : - : : - - GMT- : :	:	Sunday – Saturday
Nepali (Nepal) ne_NP	// , : Jan , : : // , : : GMT-	:	Sunday – Saturday
Nederlands (Aruba) nl_AW	28-01-2008 16:30 28 jan. 2008 16:30:05 28-01-2008 16:30:05 PST	16:30	Monday – Sunday
Nederlands (België) nl_BE	28/01/2008 16:30 28-jan-2008 16:30:05 28/01/2008 16:30:05 PST	16:30	Monday – Sunday
Nederlands (Nederland) nl_NL	28-1-2008 16:30 28-jan-2008 16:30:05 28-1-2008 16:30:05 PST	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
Nederlands (Suriname) nl_SR	28-01-2008 16:30 28 jan. 2008 16:30:05 28-01-2008 16:30:05 PST	16:30	Monday – Sunday
Norsk (Norge) no_NO	28.01.2008 16:30 28.jan.2008 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
() pa_IN	28/1/2008, 4:30 . . 28 2008, 4:30:05 . . 28/1/2008, 4:30:05 . . GMT-8	4:30 . .	Sunday – Saturday
Polski (Polska) pl_PL	28.01.2008 16:30 2008-01-28 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
Pashto (Afghanistan) ps_AF	B : / / BC Nov : : B : : / / (GMT-)	:	Saturday – Sunday
Português (Angola) pt_AO	28/01/2008, 16:30 28/01/2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Português (Brasil) pt_BR	28/01/2008 16:30 28/01/2008 16:30:05 28/01/2008 16h30min5s PST	16:30	Sunday – Saturday
Português (Cabo Verde) pt_CV	28/01/2008, 16:30 28/01/2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Português (Moçambique) pt_MZ	28/01/2008, 16:30 28/01/2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Sunday – Saturday
Português (Portugal) pt_PT	28-01-2008 16:30 28/jan/2008 16:30:05	16:30	Sunday – Saturday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28-01-2008 16:30:05 PST		
Português (São Tomé e Príncipe) pt_ST	28/01/2008, 16:30 28/01/2008, 16:30:05 28/01/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Rumantsch (Svizra) rm_CH	28-01-2008 16:30 28-01-2008 16:30:05 28-01-2008 16:30:05 GMT-8	16:30	Monday – Sunday
Rundi (Burundi) rn_BI	28/1/2008 16:30 28 Jan 2008 16:30:05 28/1/2008 16:30:05 GMT-8	16:30	Monday – Sunday
Română (Republica Moldova) ro_MD	28.01.2008, 16:30 28 ian. 2008, 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Română (România) ro_RO	28.01.2008 16:30 28.01.2008 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
Русский (Армения) ru_AM	28.01.2008 16:30 28.01.2008 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
Русский (Беларусь) ru_BY	28.01.2008, 16:30 28 янв. 2008 г., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Русский (Киргизия) ru_KG	28.01.2008, 16:30 28 янв. 2008 г., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Русский (Казахстан) ru_KZ	28.01.2008, 16:30 28 янв. 2008 г., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
Русский (Литва) ru_LT	28.01.2008 16:30 28.01.2008 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
Русский (Молдова) ru_MD	28.01.2008, 16:30 28 янв. 2008 г., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Русский (Польша) ru_PL	28.01.2008 16:30 28.01.2008 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
Русский (Россия) ru_RU	28.01.2008 16:30 28.01.2008 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
Русский (Украина) ru_UA	28.01.2008, 16:30 28 янв. 2008 г., 16:30:05 28.01.2008, 16:30:05 GMT-8	16:30	Monday – Sunday
Serbian (Latin) (Bosnia and Herzegovina) sh_BA	1/28/2008 4:30 po podne jan 28, 2008 4:30:05 po podne 1/28/2008 4:30:05 po podne GMT-8	4:30 po podne	Monday – Sunday
Serbian (Latin) (Serbia) sh_CS	1/28/2008 4:30 PM jan 28, 2008 4:30:05 PM 1/28/2008 4:30:05 PM GMT-8	4:30 PM	Monday – Sunday
Montenegrin (Montenegro) sh_ME	28.1.2008. 16.30 28.01.2008. 16.30.05 28.1.2008. 16.30.05 GMT-8	16.30	Monday – Sunday
Montenegrin (Montenegro, USD) sh_ME_USD	28.1.2008. 16.30 28.01.2008. 16.30.05 28.1.2008. 16.30.05 GMT-8	16.30	Monday – Sunday
Slovenčina (Slovensko) sk_SK	28.1.2008 16:30 28.1.2008 16:30:05	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28.1.2008 16:30:05 PST		
Slovenščina (Slovenija) sl_SI	28.1.2008 16:30 28.1.2008 16:30:05 28.1.2008 16:30:05 PST	16:30	Monday – Sunday
Samoan (United States) sm_US	1/28/2008 4:30 PM Jan 28, 2008 4:30:05 PM 1/28/2008 4:30:05 PM PST	4:30 PM	Sunday – Saturday
Samoan (Samoa) sm_WS	1/28/2008 4:30 PM Jan 28, 2008 4:30:05 PM 1/28/2008 4:30:05 PM PST	4:30 PM	Sunday – Saturday
Somali (Djibouti) so_DJ	28/01/2008 4:30 PM 28-Jan-2008 ee 4:30:05 PM 28/01/2008 4:30:05 PM GMT-8	4:30 PM	Saturday – Sunday
Somali (Somalia) so_SO	28/01/2008 4:30 PM 28-Jan-2008 ee 4:30:05 PM 28/01/2008 4:30:05 PM GMT-8	4:30 PM	Monday – Sunday
Shqip (Shqipëri) sq_AL	2008-01-28 4.30.MD 2008-01-28 4:30:05.MD 2008-01-28 4.30.05.MD PST	4.30.MD	Monday – Sunday
Serbian (Cyrillic) (Bosnia and Herzegovina) sr_BA	2008-01-28 16:30 2008-01-28 16:30:05 2008-01-28 16.30.05 PST	16:30	Monday – Sunday
Serbian (Cyrillic) (Serbia) sr_CS	28.1.2008. 16.30 28.01.2008. 16.30.05 28.1.2008. 16.30.05 PST	16.30	Monday – Sunday
Српски (Србија) sr_RS	28.1.2008. 16.30 28.01.2008. 16.30.05 28.1.2008. 16.30.05 PST	16.30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
Svenska (Sverige) sv_SE	2008-01-28 16:30 2008-jan-28 16:30:05 2008-01-28 16:30:05 PST	16:30	Monday – Sunday
Kiswahili (Kenya) sw_KE	28/01/2008 16:30 28 Jan 2008 16:30:05 28/01/2008 16:30:05 GMT -8	16:30	Sunday – Saturday
() ta_IN	28/1/2008, 4:30 28 ., 2008, 4:30:05 28/1/2008, 4:30:05 GMT-8	4:30	Sunday – Saturday
() ta_LK	28/1/2008, 16:30 28 ., 2008, 16:30:05 28/1/2008, 16:30:05 GMT-8	16:30	Monday – Sunday
() te_IN	28-01-2008 4:30 PM 28 , 2008 4:30:05 PM 28-01-2008 4:30:05 PM GMT-8	4:30 PM	Sunday – Saturday
Tajik (Tajikistan) tg_TJ	28/01/2008 16:30 28 Jan 2008 16:30:05 28/01/2008 16:30:05 GMT-8	16:30	Monday – Sunday
ไทย (ไทย) th_TH	28/1/2551, 16:30 น. 28 ม.ค. 2551, 16:30:05 28/1/2551, 16 นาฬิกา 30 นาที	16:30 น.	Sunday – Saturday
Tigrinya (Ethiopia) ti_ET	28/01/2008 4:30 PM 28 Jan 2008 4:30:05 PM 28/01/2008 4:30:05 PM GMT-8	4:30 PM	Sunday – Saturday
Tagalog (Pilipinas) tl_PH	1/28/2008 4:30 PM Jan 28, 2008 4:30:05 PM 1/28/2008 4:30:05 PM PST	4:30 PM	Sunday – Saturday
Türkçe (Türkiye) tr_TR	28.01.2008 16:30 28.Oca.2008 16:30:05	16:30	Monday – Sunday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
	28.01.2008 16:30:05 PST		
Українська (Україна) uk_UA	28.01.2008 16:30 28 січ. 2008 16:30:05 28.01.2008 16:30:05 PST	16:30	Monday – Sunday
)) ur_PK	28/1/2008 4:30 PM 28 2008 4:30:05 PM 28/1/2008 4:30:05 PM GMT -8	4:30 PM	Sunday – Saturday
Uzbek (Latin, Uzbekistan) uz_LATN_UZ	28/01/2008, 16:30 28-Jan, 2008, 16:30:05 28/01/2008, 16:30:05 (GMT-8)	16:30	Monday – Sunday
Ti ng Vi t (Vi t Nam) vi_VN	16:30 28/01/2008 16:30:05 28-01-2008 16:30:05 PST 28/01/2008	16:30	Monday – Sunday
IsiXhosa (eMzantsi Afrika) xh_ZA	2008-01-28 16:30 2008 Jan 28 16:30:05 2008-01-28 16:30:05 GMT-8	16:30	Sunday – Saturday
Yoruba (Benin) yo_BJ	28/1/2008 16:30 28 01 2008 16:30:05 28/1/2008 16:30:05 WAT-8	16:30	Monday – Sunday
中文 (中国) zh_CN	2008-1-28 下午4:30 2008-1-28 16:30:05 2008-1-28 下午04时30分05秒	下午4:30	Sunday – Saturday
中文 (中国, CNH) zh_CN_CNH	2008-1-28 下午4:30 2008-1-28 16:30:05 2008-1-28 下午04时30分05秒	下午4:30	Sunday – Saturday
中文 (中国, 拼音顺序) zh_CN_PINYIN	2008-1-28 下午4:30 2008-1-28 16:30:05 2008-1-28 下午04时30分05秒	下午4:30	Sunday – Saturday

LOCALE NAME AND CODE	DATE AND TIME FORMATS	TIME FORMAT	WEEK
中文（中国，笔画顺序） zh_CN_STROKE	2008-1-28 下午4:30 2008-1-28 16:30:05 2008-1-28 下午04时30分05秒	下午4:30	Sunday – Saturday
zh_HK	2008 1 28 4:30 2008 1 28 04:30:05 2008 1 28 04 30 05	4:30	Sunday – Saturday
() zh_HK_STROKE	2008 1 28 4:30 2008 1 28 04:30:05 2008 1 28 04 30 05	4:30	Sunday – Saturday
zh_MO	28/1/2008 4:30 2008 1 28 4:30:05 28/1/2008 4:30:05 [PST]	4:30	Sunday – Saturday
zh_MY	2008-1-28 4:30 2008-1-28 16:30:05 2008-1-28 04 30 05	4:30	Monday – Sunday
zh_SG	28/01/2008 04:30 28- -2008 04:30 28/01/2008 04:30:05	04:30	Sunday – Saturday
中文（台灣） zh_TW	2008/1/28 下午 4:30 2008/1/28 下午 04:30:05 2008/1/28 下午04時30分05秒	下午 4:30	Sunday – Saturday
中文(台灣，筆劃順序) zh_TW_STROKE	2008/1/28 下午 4:30 2008/1/28 下午 04:30:05 2008/1/28 下午04時30分05秒	下午 4:30	Sunday – Saturday
IsiZulu (iNingizimu Afrika) zu_ZA	1/28/2008 16:30 Jan 28, 2008 16:30:05 1/28/2008 16:30:05 GMT-8	16:30	Sunday – Saturday

Supported Currencies (JDK)

Salesforce supported currencies, listed by locale with Oracle's Java Development Kit (JDK) formats.

 **Note:** We recommend viewing this information in Salesforce Help. Not all characters appear correctly in PDFs.

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
Afrikaans (Suid-Afrika) af_ZA	South African Rand	ZAR	R 1 234 567,57 -R 1 234 567,57
() am_ET	Ethiopian Birr	ETB	1,234,567.57 - 1,234,567.57
)) ar_AE		AED	.. - ..
)) ar_BH		BHD	.. - ..
)) ar_DZ		DZD	.. 1.234.567,57 -.. 1.234.567,57
)) ar_EG		EGP	.. - ..
)) ar_IQ		IQD	.. - ..
)) ar_JO		JOD	.. - ..
)) ar_KW		KWD	.. - ..
)) ar_LB		LBP	.. - ..
)) ar_LY		LYD	.. 1.234.567,57 -.. 1.234.567,57
))		MAD	.. 1.234.567,57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
ar_MA			- .. 1.234.567,57
)) ar_OM		OMR	.. - ..
)) ar_QA		QAR	.. - ..
)) ar_SA		SAR	.. - ..
)) ar_SD		SDG	.. - ..
)) ar_SY		SYP	.. - ..
)) ar_TN		TND	.. 1.234.567,57 - .. 1.234.567,57
)) ar_YE		YER	.. - ..
Azerbaijani (Azerbaijan) az_AZ	Azerbaijan Manat	AZN	1.234.567,57 -1.234.567,57
Belarusian (Belarus) be_BY	Belarusian Ruble	BYN	Py61 234 567,57 -Py61 234 567,57
Български (България) bg_BG	Български лев	BGN	1234567,57 лв. -1234567,57 лв.
() bn_BD	Bangladesh Taka	BDT	., ., - ., .,
() bn_IN	Indian Rupee	INR	., ., - ., .,
Bosanski (Bosna i Hercegovina)	Convertible Marks	BAM	1.234.567,57 KM

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
bs_BA			-1.234.567,57 KM
Català (Espanya) ca_ES	Euro	EUR	€ 1.234.567,57 -€ 1.234.567,57
Čeština (Česko) cs_CZ	Česká koruna	CZK	1 234 567,57 Kč -1 234 567,57 Kč
Cymraeg (Y Deyrnas Unedig) cy_GB	British Pound	GBP	£1,234,567.57 -£1,234,567.57
Dansk (Danmark) da_DK	Krone, Danmark	DKK	kr 1.234.567,57 kr -1.234.567,57
Deutsch (Österreich) de_AT	Euro	EUR	€ 1.234.567,57 -€ 1.234.567,57
Deutsch (Belgien) de_BE	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Deutsch (Schweiz) de_CH	Schweizer Franken	CHF	SFr. 1'234'567.57 SFr.-1'234'567.57
Deutsch (Deutschland) de_DE	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Deutsch (Luxemburg) de_LU	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Dzongkha (Bhutan) dz_BT	Bhutan Ngultrum	BTN	Nu. , , . -Nu. , , .
Ελληνικά (Κύπρος) el_CY	Ευρώ	EUR	€1.234.567,57 -€1.234.567,57
Ελληνικά (Ελλάδα) el_GR	Ευρώ	EUR	1.234.567,57 € -1.234.567,57 €
English (United Arab Emirates)	UAE Dirham	AED	AED 1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
en_AE			-AED 1,234,567.57
English (Antigua & Barbuda) en_AG	East Caribbean Dollar	XCD	\$1,234,567.57 -\$1,234,567.57
English (Australia) en_AU	Australian Dollar	AUD	\$1,234,567.57 -\$1,234,567.57
English (Barbados) en_BB	Barbados Dollar	BBD	\$1,234,567.57 -\$1,234,567.57
English (Belgium) en_BE	Euro	EUR	€1,234,567.57 -€1,234,567.57
English (Bermuda) en_BM	Bermuda Dollar	BMD	\$1,234,567.57 -\$1,234,567.57
English (Bahamas) en_BS	Bahamian Dollar	BSD	\$1,234,567.57 -\$1,234,567.57
English (Botswana) en_BW	Botswana Pula	BWP	P 1,234,567.57 -P 1,234,567.57
English (Belize) en_BZ	Belize Dollar	BZD	\$1,234,567.57 -\$1,234,567.57
English (Canada) en_CA	Canadian Dollar	CAD	\$1,234,567.57 -\$1,234,567.57
English (Cameroon) en_CM	CFA Franc (BEAC)	XAF	FCFA 1,234,567.57 -FCFA 1,234,567.57
English (Cyprus) en_CY	Euro	EUR	€1,234,567.57 -€1,234,567.57
English (Germany) en_DE	Euro	EUR	€1,234,567.57 -€1,234,567.57
English (Eritrea)	Eritrea Nakfa	ERN	Nfk 1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
en_ER			-Nfk 1,234,567.57
English (Fiji) en_FJ	Fiji Dollar	FJD	\$1,234,567.57 -\$1,234,567.57
English (Falkland Islands) en_FK	Falkland Islands Pound	FKP	£1,234,567.57 -£1,234,567.57
English (United Kingdom) en_GB	British Pound	GBP	£1,234,567.57 -£1,234,567.57
English (Ghana) en_GH	Ghanaian Cedi	GHS	GH 1,234,567.57 -GH 1,234,567.57
English (Gibraltar) en_GI	Gibraltar Pound	GIP	£1,234,567.57 -£1,234,567.57
English (Gambia) en_GM	Gambian Dalasi	GMD	D 1,234,567.57 -D 1,234,567.57
English (Guyana) en_GY	Guyana Dollar	GYD	\$1,234,567.57 -\$1,234,567.57
English (Hong Kong SAR China) en_HK	Hong Kong Dollar	HKD	HK\$1,234,567.57 -HK\$1,234,567.57
English (Indonesia) en_ID	Indonesian Rupiah	IDR	IDR1,234,567.57 -IDR1,234,567.57
English (Ireland) en_IE	Euro	EUR	€1,234,567.57 -€1,234,567.57
English (Israel) en_IL	Israeli Shekel	ILS	1,234,567.57 - 1,234,567.57
English (India) en_IN	Indian Rupee	INR	12,34,567.57 - 12,34,567.57
English (Italy)	Euro	EUR	€1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
en_IT			-€1,234,567.57
English (Jamaica) en_JM	Jamaican Dollar	JMD	\$1,234,567.57 -\$1,234,567.57
English (Kenya) en_KE	Kenyan Shilling	KES	Ksh 1,234,567.57 -Ksh 1,234,567.57
English (Cayman Islands) en_KY	Cayman Islands Dollar	KYD	\$1,234,567.57 -\$1,234,567.57
English (Liberia) en_LR	Liberian Dollar	LRD	\$1,234,567.57 -\$1,234,567.57
English (Madagascar) en_MG	Malagasy Ariary	MGA	Ar 1,234,567.57 -Ar 1,234,567.57
English (Malta) en_MT	Euro	EUR	€1,234,567.57 -€1,234,567.57
English (Mauritius) en_MU	Mauritius Rupee	MUR	Rs 1,234,567.57 -Rs 1,234,567.57
English (Malawi) en_MW	Malawi Kwacha	MWK	MK 1,234,567.57 -MK 1,234,567.57
English (Malaysia) en_MY	Malaysian Ringgit	MYR	RM 1,234,567.57 -RM 1,234,567.57
English (Namibia) en_NA	Namibian Dollar	NAD	\$1,234,567.57 -\$1,234,567.57
English (Nigeria) en_NG	Nigerian Naira	NGN	1,234,567.57 -1,234,567.57
English (Netherlands) en_NL	Euro	EUR	€1,234,567.57 -€1,234,567.57
English (New Zealand)	New Zealand Dollar	NZD	\$1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
en_NZ			-\$1,234,567.57
English (Papua New Guinea) en_PG	Papua New Guinea Kina	PGK	K 1,234,567.57 -K 1,234,567.57
English (Philippines) en_PH	Philippine Peso	PHP	Php1,234,567.57 (Php1,234,567.57)
English (Pakistan) en_PK	Pakistani Rupee	PKR	Rs 1,234,567.57 -Rs 1,234,567.57
English (Rwanda) en_RW	Rwanda Franc	RWF	RF 1,234,567.57 -RF 1,234,567.57
English (Solomon Islands) en_SB	Solomon Islands Dollar	SBD	\$1,234,567.57 -\$1,234,567.57
English (Seychelles) en_SC	Seychelles Rupee	SCR	SR 1,234,567.57 -SR 1,234,567.57
English (Singapore) en_SG	Singapore Dollar	SGD	\$1,234,567.57 -\$1,234,567.57
English (St. Helena) en_SH	St Helena Pound	SHP	£1,234,567.57 -£1,234,567.57
English (Sierra Leone) en_SL	Sierra Leone Leone	SLE	SLE 1,234,567.57 -SLE 1,234,567.57
English (Sierra Leone, SLL) en_SL_SLL	Sierra Leone Leone	SLL	Le 1,234,567.57 -Le 1,234,567.57
English (Sint Maarten) en_SX	Neth Antilles Guilder	ANG	NAf. 1,234,567.57 -NAf. 1,234,567.57
English (Eswatini) en_SZ	Eswatini Lilageni	SZL	E 1,234,567.57 -E 1,234,567.57
English (Tonga) en_TO	Tonga Pa'anga	TOP	T\$1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
en_TO			-T\$1,234,567.57
English (Trinidad & Tobago) en_TT	Trinidad&Tobago Dollar	TTD	\$1,234,567.57 -\$1,234,567.57
English (Tanzania) en_TZ	Tanzanian Shilling	TZS	TSh 1,234,567.57 -TSh 1,234,567.57
English (Uganda) en_UG	Ugandan Shilling	UGX	USh 1,234,567.57 -USh 1,234,567.57
English (United States) en_US	U.S. Dollar	USD	\$1,234,567.57 (\$1,234,567.57)
English (Vanuatu) en_VU	Vanuatu Vatu	VUV	VT 1,234,567.57 -VT 1,234,567.57
English (Samoa) en_WS	Samoa Tala	WST	WS\$1,234,567.57 -WS\$1,234,567.57
English (South Africa) en_ZA	South African Rand	ZAR	R 1,234,567.57 R-1,234,567.57
Español (Argentina) es_AR	Peso argentino	ARS	\$1.234.567,57 \$-1.234.567,57
Español (Bolivia) es_BO	Boliviano de Bolivia	BOB	B\$1.234.567,57 (B\$1.234.567,57)
Español (Chile) es_CL	Peso chileno	CLP	Ch\$1.234.567,57 Ch\$-1.234.567,57
Español (Colombia) es_CO	Peso colombiano	COP	\$1.234.567,57 (\$1.234.567,57)
Español (Costa Rica) es_CR	Colón costarricense	CRC	C1,234,567.57 (C1,234,567.57)
Español (Cuba)	Peso cubano	CUP	\$1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
es_CU			-\$1,234,567.57
Español (República Dominicana) es_DO	Peso dominicano	DOP	RD\$1,234,567.57 (RD\$1,234,567.57)
Español (Ecuador) es_EC	Dólar estadounidense	USD	\$1.234.567,57 \$-1.234.567,57
Español (España) es_ES	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Español (Guatemala) es_GT	Quetzal guatemalteco	GTQ	Q1,234,567.57 (Q1,234,567.57)
Español (Honduras) es_HN	Lempira hondureño	HNL	L1,234,567.57 (L1,234,567.57)
Español (México) es_MX	Peso mexicano	MXN	\$1,234,567.57 -\$1,234,567.57
Español (Nicaragua) es_NI	Córdoba nicaragüense	NIO	₡C1,234,567.57 (₡C1,234,567.57)
Español (Panamá) es_PA	Balboa panameño	PAB	B1,234,567.57 (B1,234,567.57)
Español (Perú) es_PE	Sol peruano	PEN	S/ 1,234,567.57 -S/ 1,234,567.57
Español (Puerto Rico) es_PR	Dólar estadounidense	USD	\$1,234,567.57 (\$1,234,567.57)
Español (Paraguay) es_PY	Guaraní paraguayo	PYG	G1.234.567,57 (G1.234.567,57)
Español (El Salvador) es_SV	Colón salvadoreño	SVC	C1,234,567.57 (C1,234,567.57)
Español (Estados Unidos)	Dólar estadounidense	USD	US\$1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
es_US			(US\$1,234,567.57)
Español (Uruguay) es_UY	Peso uruguayo	UYU	NU\$ 1.234.567,57 (NU\$1.234.567,57)
Español (Venezuela) es_VE	Bolívar soberano venezolano	VES	Bs.S.1.234.567,57 Bs.S. -1.234.567,57
Eesti (Eesti) et_EE	Euro	EUR	1 234 567,57 € -1 234 567,57 €
Euskara (Españia) eu_ES	Euro	EUR	1.234.567,57 € -1.234.567,57 €
فارسی (ایران) fa_IR	Iranian Rial	IRR	—
Suomi (Suomi) fi_FI	Euro	EUR	1 234 567,57 € -1 234 567,57 €
Français (Belgique) fr_BE	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Français (Canada) fr_CA	Dollar canadien	CAD	1 234 567,57 \$ (1 234 567,57\$)
Français (Suisse) fr_CH	Franc suisse	CHF	SFr. 1'234'567.57 SFr.-1'234'567.57
Français (France) fr_FR	Euro	EUR	1 234 567,57 € -1 234 567,57 €
Français (Guinée) fr_GN	Franc guinéen	GNF	1 234 567,57 FG -1 234 567,57 FG
Français (Haïti) fr_HT	Gourde Haïtienne	HTG	1 234 567,57 G -1 234 567,57 G
Français (Comores) fr_KM	Franc comorien	KMF	1 234 567,57 CF

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
fr_KM			-1 234 567,57 CF
Français (Luxembourg) fr_LU	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Français (Maroc) fr_MA	Dirham marocain	MAD	1.234.567,57 MAD -1.234.567,57 MAD
Français (Monaco) fr_MC	Euro	EUR	1 234 567,57 € -1 234 567,57 €
Français (Mauritanie) fr_MR	Ougulya mauritanien	MRU	1 234 567,57 UM -1 234 567,57 UM
Français (Wallis-et-Futuna) fr_WF	Franc du Pacifique	XPF	1 234 567,57 FCFP -1 234 567,57 FCFP
Gaeilge (Éire) ga_IE	Euro	EUR	€1,234,567.57 -€1,234,567.57
() gu_IN	Indian Rupee	INR	12,34,567.57 - 12,34,567.57
Ōlelo Hawai i (Amelika Hui Pū la) haw_US	U.S. Dollar	USD	\$1,234,567.57 -\$1,234,567.57
() hi_IN	Indian Rupee	INR	12,34,567.57 - 12,34,567.57
Hmong (United States) hmn_US	U.S. Dollar	USD	USD 1,234,567.57 -USD 1,234,567.57
Hrvatski (Hrvatska) hr_HR	ero	EUR	€ 1.234.567,57 -€ 1.234.567,57
Hrvatski (Hrvatska, HRK) hr_HR_HRK	kuna	HRK	Kn 1.234.567,57 -Kn 1.234.567,57
Haitian Creole (Haiti)	Gourde Haïtienne	HTG	HTG 1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
ht_HT			-HTG 1,234,567.57
Haitian Creole (United States) ht_US	Dollar américain	USD	USD 1,234,567.57 -USD 1,234,567.57
Magyar (Magyarország) hu_HU	Magyar forint	HUF	1 234 567,57 Ft -1 234 567,57 Ft
() hy_AM	Armenian Dram	AMD	1 234 567,57 -1 234 567,57
Indonesia (Indonesia) in_ID	Rupiah Indonesia	IDR	Rp1.234.567,57 -Rp1.234.567,57
Íslenska (Ísland) is_IS	Iceland Krona	ISK	1.234.567,57 kr. -1.234.567,57 kr.
Italiano (Svizzera) it_CH	Franco (Svizzero)	CHF	SFr. 1'234'567.57 SFr.-1'234'567.57
Italiano (Italia) it_IT	Euro	EUR	€ 1.234.567,57 -€ 1.234.567,57
() iw_IL		ILS	1,234,567.57 " -1,234,567.57 "
日本語 (日本) ja_JP	日本円	JPY	¥ 1,234,567.57 - ¥ 1,234,567.57
Yiddish (United States) ji_US	U.S. Dollar	USD	\$1,234,567.57 -\$1,234,567.57
() ka_GE	Georgia Lari	GEL	1 234 567,57 -1 234 567,57
аза тілі (азастан) kk_KZ	Kazakhstan Tenge	KZT	1 234 567,57 -1 234 567,57
Kalaallisut (Kalaallit Nunaat)	Danish Krone	DKK	kr. 1.234.567,57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
kl_GL			kr.-1.234.567,57
() km_KH	Cambodia Riel	KHR	1.234.567,57 -1.234.567,57
() kn_IN	Indian Rupee	INR	1,234,567.57 - 1,234,567.57
한국어 (북한) ko_KP	조선민주주의인민공화국 원	KPW	KPW 1,234,567.57 -KPW1,234,567.57
한국어 (대한민국) ko_KR	대한민국 원	KRW	₩1,234,567.57 -₩1,234,567.57
Kyrgyz (Kyrgyzstan) ky_KG	Kyrgyzstan Som	KGS	1 234 567,57 com -1 234 567,57 com
Lëtzebuergesch (Lëtzebuerg) lb_LU	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Lao (Laos) lo_LA	Lao Kip	LAK	1.234.567,57 -1.234.567,57
Lietuvių (Lietuva) lt_LT	Euro	EUR	1 234 567,57 € -1 234 567,57 €
Luba-Katanga (Congo - Kinshasa) lu_CD	Franc Congolais	CDF	1.234.567,57 FC -1.234.567,57 FC
Latviešu (Latvija) lv_LV	Euro	EUR	1 234 567,57 € -1 234 567,57 €
Te reo (New Zealand) mi_NZ	New Zealand Dollar	NZD	\$ 1,234,567.57 -\$ 1,234,567.57
Македонски (Северна Македонија) mk_MK	Macedonian Denar	MKD	Den 1.234.567,57 -Den 1.234.567,57
()	Indian Rupee	INR	1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
ml_IN			- 1,234,567.57
() mr_IN	Indian Rupee	INR	, , . - , , .
Melayu (Brunei) ms_BN	Dolar Brunei	BND	\$ 1.234.567,57 -\$ 1.234.567,57
Melayu (Malaysia) ms_MY	Ringgit Malaysia	MYR	RM1,234,567.57 (RM1,234,567.57)
Malti (Malta) mt_MT	Euro	EUR	€1,234,567.57 -€1,234,567.57
() my_MM	Myanmar Kyat	MMK	, , . K - , , . K
Nepali (Nepal) ne_NP	Nepalese Rupee	NPR	, , . - , , .
Nederlands (Aruba) nl_AW	Arubaanse gulden	AWG	Afl. 1.234.567,57 Afl. -1.234.567,57
Nederlands (België) nl_BE	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Nederlands (Nederland) nl_NL	Euro	EUR	€ 1.234.567,57 € 1.234.567,57-
Nederlands (Suriname) nl_SR	Surinaamse dollar	SRD	\$ 1.234.567,57 \$ -1.234.567,57
Norsk (Norge) no_NO	Norsk krone	NOK	kr 1 234 567,57 kr -1 234 567,57
() pa_IN	Indian Rupee	INR	12,34,567.57 - 12,34,567.57
Polski (Polska)	Złoty polski	PLN	1 234 567,57 zł

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
pl_PL			-1 234 567,57 zł
Pashto (Afghanistan) ps_AF	Afghanistan Afghani (New)	AFN	-
Português (Angola) pt_AO	Kwanza Angolano	AOA	1 234 567,57 Kz -1 234 567,57 Kz
Português (Brasil) pt_BR	Real brasileiro	BRL	R\$ 1.234.567,57 -R\$ 1.234.567,57
Português (Cabo Verde) pt_CV	Escudo de Cabo Verde	CVE	1 234 567\$57 -1 234 567\$57
Português (Moçambique) pt_MZ	Novo Metical Moçambicano	MZN	1 234 567,57 MTn -1 234 567,57 MTn
Português (Portugal) pt_PT	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Português (São Tomé e Príncipe) pt_ST	Dobra de São Tomé e Príncipe	STN	1 234 567,57 Db -1 234 567,57 Db
Rumantsch (Svizra) rm_CH	Swiss Franc	CHF	1'234'567.57 CHF -1'234'567.57 CHF
Rundi (Burundi) rn_BI	Burundi Franc	BIF	1.234.567,57 FBu -1.234.567,57 FBu
Română (Republica Moldova) ro_MD	Leu moldovenesc	MDL	1.234.567,57 L -1.234.567,57 L
Română (România) ro_RO	Leu românesc	RON	1.234.567,57 LEI -1.234.567,57 LEI
Русский (Армения) ru_AM	Армянский драм	AMD	AMD 1 234 567,57 -AMD 1 234 567,57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
Русский (Беларусь) ru_BY	Белорусский рубль	BYN	1 234 567,57 Br -1 234 567,57 Br
Русский (Киргизия) ru_KG	Киргизский сом	KGS	1 234 567,57 сом -1 234 567,57 сом
Русский (Казахстан) ru_KZ	Казахстанский тенге	KZT	1 234 567,57 ₸ -1 234 567,57 ₸
Русский (Литва) ru_LT	Евро	EUR	€ 1 234 567,57 -€ 1 234 567,57
Русский (Молдова) ru_MD	Молдавский лей	MDL	1 234 567,57 L -1 234 567,57 L
Русский (Польша) ru_PL	Польский злотый	PLN	PLN 1 234 567,57 -PLN 1 234 567,57
Русский (Россия) ru_RU	Российский рубль	RUB	1 234 567,57 руб. -1 234 567,57 руб.
Русский (Украина) ru_UA	Украинская гривна	UAH	1 234 567,57 ₴ -1 234 567,57 ₴
Serbian (Latin) (Bosnia and Herzegovina) sh_BA	Convertible Marks	BAM	1.234.567,57 KM -1.234.567,57 KM
Serbian (Latin) (Serbia) ¹ sh_CS	Serbian Dinar	CSD	1.234.567,57 CSD -1.234.567,57 CSD
Montenegrin (Montenegro) sh_ME	Euro	EUR	1.234.567,57 € -1.234.567,57 €
Montenegrin (Montenegro, USD) sh_ME_USD	U.S. Dollar	USD	¤1,234,567.57 (¤1,234,567.57)
Slovenčina (Slovensko) sk_SK	Euro	EUR	1 234 567,57 € -1 234 567,57 €

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
Slovenščina (Slovenija) sl_SI	Evro	EUR	€ 1.234.567,57 -€ 1.234.567,57
Samoan (United States) sm_US	U.S. Dollar	USD	USD 1,234,567.57 -USD 1,234,567.57
Samoan (Samoa) sm_WS	Samoa Tala	WST	WST 1,234,567.57 -WST 1,234,567.57
Somali (Djibouti) so_DJ	Djibouti Franc	DJF	Fdj 1,234,567.57 -Fdj 1,234,567.57
Somali (Somalia) so_SO	Somali Shilling	SOS	S 1,234,567.57 -S 1,234,567.57
Shqip (Shqipëri) sq_AL	Albanian Lek	ALL	Lek1.234.567,57 -Lek1.234.567,57
Serbian (Cyrillic) (Bosnia and Herzegovina) sr_BA	Convertible Marks	BAM	KM. 1.234.567,57 -KM. 1.234.567,57
Serbian (Cyrillic) (Serbia) ¹ sr_CS	Serbian Dinar	CSD	CSD 1.234.567,57 -CSD 1.234.567,57
Српски (Србија) sr_RS	Serbian Dinar	RSD	дин. 1.234.567,57 -дин. 1.234.567,57
Svenska (Sverige) sv_SE	Sverige Krona	SEK	1 234 567,57 kr -1 234 567,57 kr
Kiswahili (Kenya) sw_KE	Kenyan Shilling	KES	Ksh 1,234,567.57 -Ksh 1,234,567.57
() ta_IN	Indian Rupee	INR	12,34,567.57 - 12,34,567.57
() ta_LK	Sri Lanka Rupee	LKR	Rs. 12,34,567.57 -Rs. 12,34,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
() te_IN	Indian Rupee	INR	12,34,567.57 - 12,34,567.57
Tajik (Tajikistan) tg_TJ	Tajik Somoni	TJS	1 234 567,57 сом. -1 234 567,57 сом.
ไทย (ไทย) th_TH	บาท ไทย	THB	฿1,234,567.57 ฿-1,234,567.57
Tigrinya (Ethiopia) ti_ET	Ethiopian Birr	ETB	Br 1,234,567.57 -Br 1,234,567.57
Tagalog (Pilipinas) tl_PH	Philippine Peso	PHP	PHP 1,234,567.57 -PHP 1,234,567.57
Türkçe (Türkiye) tr_TR	Türk Lirası (Yeni)	TRY	1.234.567,57 TL -1.234.567,57 TL
Українська (Україна) uk_UA	Українська гривня	UAH	1 234 567,57 грн. -1 234 567,57 грн.
()) ur_PK	Pakistani Rupee	PKR	Rs 1,234,567.57 -Rs 1,234,567.57
Uzbek (Latin, Uzbekistan) uz_LATN_UZ	Uzbekistan Sum	UZS	1 234 567,57 so m -1 234 567,57 so m
Ti ng Vi t (Vi t Nam) vi_VN	Đô ng Vi t Nam	VND	1.234.567,57 đ -1.234.567,57 đ
IsiXhosa (eMzantsi Afrika) xh_ZA	South African Rand	ZAR	R 1 234 567.57 -R 1 234 567.57
Yoruba (Benin) yo_BJ	CFA Franc (BCEAO)	XOF	F CFA 1,234,567.57 -F CFA 1,234,567.57
中文 (中国) zh_CN	中国人民币	CNY	¥1,234,567.57 -¥1,234,567.57

LOCALE NAME AND CODE	DEFAULT CURRENCY	CURRENCY CODE	CURRENCY FORMAT
中文（中国，CNH） zh_CN_CNH	中国人民币（离岸）	CNH	CNH1,234,567.57 -CNH1,234,567.57
中文（中国，拼音顺序） zh_CN_PINYIN	中国人民币	CNY	¥1,234,567.57 -¥1,234,567.57
中文（中国，笔画顺序） zh_CN_STROKE	中国人民币	CNY	¥1,234,567.57 -¥1,234,567.57
zh_HK		HKD	HK\$1,234,567.57 (HK\$1,234,567.57)
() zh_HK_STROKE		HKD	HK\$1,234,567.57 (HK\$1,234,567.57)
zh_MO		MOP	MOP\$1,234,567.57 -MOP\$1,234,567.57
zh_MY		MYR	MYR 1,234,567.57 -MYR 1,234,567.57
zh_SG		SGD	S\$1,234,567.57 -S\$1,234,567.57
中文（台灣） zh_TW	台幣	TWD	NT\$1,234,567.57 -NT\$1,234,567.57
中文（台灣，筆劃順序） zh_TW_STROKE	台幣	TWD	NT\$1,234,567.57 -NT\$1,234,567.57
IsiZulu (iNingizimu Afrika) zu_ZA	South African Rand	ZAR	R 1,234,567.57 -R 1,234,567.57

¹ The CSD currency is only available in single currency orgs and orgs that activated multiple currencies when CSD was the corporate currency. It represents the old Serbian Dinar used in Serbia and Montenegro from 2003 to 2006. Because it's no longer a valid ISO currency code, it can be incompatible with other systems. If your org uses this currency, we recommend moving to the current Serbian Dinar currency, RSD. The corresponding locale is Serbian (Serbia) with the sr_RS locale code.

Set Your Personal or Organization-Wide Currency

If you have a single-currency organization, you can set the default currency for your organization. Multi-currency organizations don't have a default currency. Instead, change your corporate currency or your personal currency.

[Set Your Currency Locale](#)

If you have a single-currency organization, you can set your default currency.

[Set Your Corporate Currency](#)

In multi-currency organizations, set your corporate currency to the currency in which your corporate headquarters reports revenue. All conversion rates are based on the corporate currency.

[Set Your Personal Currency](#)

In multi-currency organizations, you can set a personal currency that's different from the organization's corporate currency.

SEE ALSO:

[Language, Locale, and Currency Settings](#)

[Edit Conversion Rates](#)

[Supported Currencies \(ICU\)](#)

[Supported Number, Name, and Address Formats \(ICU\)](#)

Set Your Currency Locale

If you have a single-currency organization, you can set your default currency.

1. Search Setup for Company Information.
2. On the Company Information page, click **Edit**.
3. Select a locale from the Currency Locale drop-down list.
4. Click **Save**.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience.

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To view currencies:

- View Setup and Configuration

To change currencies:

- Customize Application

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience.

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To view currencies:

- View Setup and Configuration

To change currencies:

- Customize Application

Set Your Corporate Currency

In multi-currency organizations, set your corporate currency to the currency in which your corporate headquarters reports revenue. All conversion rates are based on the corporate currency.

When Support enables multiple currencies, your corporate currency is set to the value specified on the Company Information page in Setup. You can change the corporate currency.

1. Search Setup for Manage Currencies.
2. On the Currency page, click **Change Corporate**.
3. Select a currency from the New Corporate Currency drop-down list.
4. Click **Save**.

Set Your Personal Currency

In multi-currency organizations, you can set a personal currency that's different from the organization's corporate currency.

1. From your personal settings, enter *Time Zone* in the Quick Find box, then select **Language and Time Zone**. No results? Enter *Personal Information* in the Quick Find box, then select **Personal Information**.
2. Select a currency from the Currency drop-down list.
3. Save your changes.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience.

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To view currencies:

- View Setup and Configuration

To change currencies:

- Customize Application

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To view company information:

- View Setup and Configuration

To change company information:

- Customize Application

The available personal setup options vary according to which Salesforce Edition you have.

Edit Conversion Rates

You can manage static exchange rates between your active and inactive currencies and the corporate currency by editing the conversion rates. These exchange rates apply to all currency fields used in your organization. In addition to these conversion rates, some organizations use dated exchange rates for opportunities and opportunity products.

1. Search Setup for Manage Currencies.
2. If you use advanced currency management, click **Manage Currencies**.
3. In the Active Currencies or Inactive Currencies list, click **Edit Rates**.
4. Enter the conversion rate between each currency and your corporate currency.
5. Click **Save**.

When you change the conversion rates, currency amounts are updated using the new rates. Previous conversion rates are not stored. All conversions within opportunities, forecasts, and other amounts use the current conversion rate.

If your organization uses advanced currency management, you can also manage dated exchange rates for currency fields on opportunities and opportunity products.

Note:

- You cannot track revenue gain or loss based on currency fluctuations.
- Changing conversion rates causes a mass recalculation of roll-up summary fields. This recalculation can take up to 30 minutes, depending on the number of records affected.
- You can also change a conversion rate via the API. However, if another roll-up summary recalculation for the same currency field is in progress, the age of that job affects the recalculation job that you triggered. Here's what happens when you request a currency rate change via the API, and a related job is in progress.
 - If the other recalculation for the same currency field was kicked off less than 24 hours ago, your currency rate change isn't saved. You can try again later or instead change the currency rate from Manage Currencies in Setup. Initiating the change from Setup stops the old job and triggers your recalculation to run.
 - If the other recalculation job was kicked off more than 24 hours ago, you can save your currency rate change and your job starts.

To check the status of your recalculation job, see the Background Jobs page in Setup.

SEE ALSO:

[Set Your Personal or Organization-Wide Currency](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To view currencies:

- View Setup and Configuration

To change currencies:

- Customize Application

Supported Time Zones

You can find a list of Salesforce supported time zones and codes for your organization under your personal settings.

- From your personal settings, enter *Time Zone* in the Quick Find box, then select **Language and Time Zone**. No results? Enter *Personal Information* in the Quick Find box, then select **Personal Information**. Then click **Edit**.
- Click the Time Zone dropdown list for a list of supported time zones.

For reference, here are the Salesforce supported times zones and codes.

TIME ZONE CODE	TIME ZONE NAME
GMT+14:00	Line Islands Time (Pacific/Kiritimati)
GMT+13:00	Apia Standard Time (Pacific/Apia)
GMT+13:00	Phoenix Islands Time (Pacific/Enderbury)
GMT+13:00	Tokelau Time (Pacific/Fakaofu)
GMT+13:00	Tonga Standard Time (Pacific/Tongatapu)
GMT+12:45	Chatham Standard Time (Pacific/Chatham)
GMT+13:45	Chatham Daylight Time (Pacific/Chatham)
GMT+12:00	New Zealand Standard Time (Antarctica/McMurdo)
GMT+13:00	New Zealand Daylight Time (Antarctica/McMurdo)
GMT+12:00	Anadyr Standard Time (Asia/Anadyr)
GMT+12:00	Petropavlovsk-Kamchatski Standard Time (Asia/Kamchatka)
GMT+12:00	New Zealand Standard Time (Pacific/Auckland)
GMT+13:00	New Zealand Daylight Time (Pacific/Auckland)
GMT+12:00	Fiji Standard Time (Pacific/Fiji)
GMT+12:00	Tuvalu Time (Pacific/Funafuti)
GMT+12:00	Marshall Islands Time (Pacific/Kwajalein)
GMT+12:00	Marshall Islands Time (Pacific/Majuro)
GMT+12:00	Nauru Time (Pacific/Nauru)
GMT+12:00	Gilbert Islands Time (Pacific/Tarawa)
GMT+12:00	Wake Island Time (Pacific/Wake)
GMT+12:00	Wallis & Futuna Time (Pacific/Wallis)
GMT+11:00	Casey Time (Antarctica/Casey)
GMT+11:00	Magadan Standard Time (Asia/Magadan)

EDITIONS

Available in: Lightning Experience and Salesforce Classic ([not available in all orgs](#))

Available in: **Group, Professional, Enterprise, Performance, Unlimited, Database.com,** and **Developer** Editions

USER PERMISSIONS

To view company information:

- View Setup and Configuration

To change company information:

- Customize Application

The available personal setup options vary according to which Salesforce edition you have.

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT+11:00	Sakhalin Standard Time (Asia/Sakhalin)
GMT+11:00	Magadan Standard Time (Asia/Srednekolymsk)
GMT+11:00	Bougainville Standard Time (Pacific/Bougainville)
GMT+11:00	Vanuatu Standard Time (Pacific/Efate)
GMT+11:00	Solomon Islands Time (Pacific/Guadalcanal)
GMT+11:00	Kosrae Time (Pacific/Kosrae)
GMT+11:00	Norfolk Island Standard Time (Pacific/Norfolk)
GMT+12:00	Norfolk Island Daylight Time (Pacific/Norfolk)
GMT+11:00	New Caledonia Standard Time (Pacific/Noumea)
GMT+11:00	Ponape Time (Pacific/Ponape)
GMT+10:30	Lord Howe Standard Time (Australia/Lord_Howe)
GMT+11:00	Lord Howe Daylight Time (Australia/Lord_Howe)
GMT+10:00	Dumont-d'Urville Time (Antarctica/DumontDUrville)
GMT+10:00	Australian Eastern Standard Time (Antarctica/Macquarie)
GMT+11:00	Australian Eastern Daylight Time (Antarctica/Macquarie)
GMT+10:00	Vladivostok Standard Time (Asia/Ust-Nera)
GMT+10:00	Vladivostok Standard Time (Asia/Vladivostok)
GMT+10:00	Australian Eastern Standard Time (Australia/Brisbane)
GMT+10:00	Australian Eastern Standard Time (Australia/Currie)
GMT+11:00	Australian Eastern Daylight Time (Australia/Currie)
GMT+10:00	Australian Eastern Standard Time (Australia/Hobart)
GMT+11:00	Australian Eastern Daylight Time (Australia/Hobart)
GMT+10:00	Australian Eastern Standard Time (Australia/Lindeman)
GMT+10:00	Australian Eastern Standard Time (Australia/Melbourne)
GMT+11:00	Australian Eastern Daylight Time (Australia/Melbourne)
GMT+10:00	Australian Eastern Standard Time (Australia/Sydney)
GMT+11:00	Australian Eastern Daylight Time (Australia/Sydney)
GMT+10:00	Chamorro Standard Time (Pacific/Guam)
GMT+10:00	Papua New Guinea Time (Pacific/Port_Moresby)
GMT+10:00	Chamorro Standard Time (Pacific/Saipan)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT+10:00	Chuuk Time (Pacific/Truk)
GMT+09:30	Australian Central Standard Time (Australia/Adelaide)
GMT+10:30	Australian Central Daylight Time (Australia/Adelaide)
GMT+09:30	Australian Central Standard Time (Australia/Broken_Hill)
GMT+10:30	Australian Central Daylight Time (Australia/Broken_Hill)
GMT+09:30	Australian Central Standard Time (Australia/Darwin)
GMT+09:00	Yakutsk Standard Time (Asia/Chita)
GMT+09:00	East Timor Time (Asia/Dili)
GMT+09:00	Eastern Indonesia Time (Asia/Jayapura)
GMT+09:00	Yakutsk Standard Time (Asia/Khandyga)
GMT+09:00	Korean Standard Time (Asia/Pyongyang)
GMT+09:00	Korean Standard Time (Asia/Seoul)
GMT+09:00	Japan Standard Time (Asia/Tokyo)
GMT+09:00	Yakutsk Standard Time (Asia/Yakutsk)
GMT+09:00	Palau Time (Pacific/Palau)
GMT+08:45	Australian Central Western Standard Time (Australia/Eucla)
GMT+08:00	Brunei Darussalam Time (Asia/Brunei)
GMT+08:00	Ulaanbaatar Standard Time (Asia/Choibalsan)
GMT+08:00	Hong Kong Standard Time (Asia/Hong_Kong)
GMT+08:00	Irkutsk Standard Time (Asia/Irkutsk)
GMT+08:00	Malaysia Time (Asia/Kuala_Lumpur)
GMT+08:00	Malaysia Time (Asia/Kuching)
GMT+08:00	China Standard Time (Asia/Macau)
GMT+08:00	Central Indonesia Time (Asia/Makassar)
GMT+08:00	Philippine Standard Time (Asia/Manila)
GMT+08:00	China Standard Time (Asia/Shanghai)
GMT+08:00	Singapore Standard Time (Asia/Singapore)
GMT+08:00	Taipei Standard Time (Asia/Taipei)
GMT+08:00	Ulaanbaatar Standard Time (Asia/Ulaanbaatar)
GMT+08:00	Australian Western Standard Time (Australia/Perth)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT+07:00	Davis Time (Antarctica/Davis)
GMT+07:00	Indochina Time (Asia/Bangkok)
GMT+07:00	Moscow Standard Time + 4 (Asia/Barnaul)
GMT+07:00	Indochina Time (Asia/Ho_Chi_Minh)
GMT+07:00	Hovd Standard Time (Asia/Hovd)
GMT+07:00	Western Indonesia Time (Asia/Jakarta)
GMT+07:00	Krasnoyarsk Standard Time (Asia/Krasnoyarsk)
GMT+07:00	Krasnoyarsk Standard Time (Asia/Novokuznetsk)
GMT+07:00	Novosibirsk Standard Time (Asia/Novosibirsk)
GMT+07:00	Indochina Time (Asia/Phnom_Penh)
GMT+07:00	Western Indonesia Time (Asia/Pontianak)
GMT+07:00	Moscow Standard Time + 4 (Asia/Tomsk)
GMT+07:00	Indochina Time (Asia/Vientiane)
GMT+07:00	Christmas Island Time (Indian/Christmas)
GMT+06:30	Myanmar Time (Asia/Rangoon)
GMT+06:30	Cocos Islands Time (Indian/Cocos)
GMT+06:00	Vostok Time (Antarctica/Vostok)
GMT+06:00	East Kazakhstan Time (Asia/Almaty)
GMT+06:00	Kyrgyzstan Time (Asia/Bishkek)
GMT+06:00	Bangladesh Standard Time (Asia/Dhaka)
GMT+06:00	Omsk Standard Time (Asia/Omsk)
GMT+06:00	East Kazakhstan Time (Asia/Qostanay)
GMT+06:00	Bhutan Time (Asia/Thimphu)
GMT+06:00	China Standard Time (Asia/Urumqi)
GMT+06:00	Indian Ocean Time (Indian/Chagos)
GMT+05:45	Nepal Time (Asia/Kathmandu)
GMT+05:30	India Standard Time (Asia/Colombo)
GMT+05:30	India Standard Time (Asia/Kolkata)
GMT+05:00	Mawson Time (Antarctica/Mawson)
GMT+05:00	West Kazakhstan Time (Asia/Aqtau)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT+05:00	West Kazakhstan Time (Asia/Aqtobe)
GMT+05:00	Turkmenistan Standard Time (Asia/Ashgabat)
GMT+05:00	West Kazakhstan Time (Asia/Atyrau)
GMT+05:00	Tajikistan Time (Asia/Dushanbe)
GMT+05:00	Pakistan Standard Time (Asia/Karachi)
GMT+05:00	West Kazakhstan Time (Asia/Oral)
GMT+05:00	West Kazakhstan Time (Asia/Qyzylorda)
GMT+05:00	Uzbekistan Standard Time (Asia/Samarkand)
GMT+05:00	Uzbekistan Standard Time (Asia/Tashkent)
GMT+05:00	Yekaterinburg Standard Time (Asia/Yekaterinburg)
GMT+05:00	French Southern & Antarctic Time (Indian/Kerguelen)
GMT+05:00	Maldives Time (Indian/Maldives)
GMT+04:30	Afghanistan Time (Asia/Kabul)
GMT+04:00	Azerbaijan Standard Time (Asia/Baku)
GMT+04:00	Gulf Standard Time (Asia/Dubai)
GMT+04:00	Gulf Standard Time (Asia/Muscat)
GMT+04:00	Georgia Standard Time (Asia/Tbilisi)
GMT+04:00	Armenia Standard Time (Asia/Yerevan)
GMT+04:00	Samara Standard Time (Europe/Astrakhan)
GMT+04:00	Samara Standard Time (Europe/Samara)
GMT+04:00	Moscow Standard Time + 1 (Europe/Saratov)
GMT+04:00	Moscow Standard Time + 1 (Europe/Ulyanovsk)
GMT+04:00	Seychelles Time (Indian/Mahe)
GMT+04:00	Mauritius Standard Time (Indian/Mauritius)
GMT+04:00	Réunion Time (Indian/Reunion)
GMT+03:30	Iran Standard Time (Asia/Tehran)
GMT+03:00	East Africa Time (Africa/Addis_Ababa)
GMT+03:00	East Africa Time (Africa/Asmera)
GMT+03:00	East Africa Time (Africa/Dar_es_Salaam)
GMT+03:00	East Africa Time (Africa/Djibouti)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT+03:00	East Africa Time (Africa/Kampala)
GMT+03:00	East Africa Time (Africa/Mogadishu)
GMT+03:00	East Africa Time (Africa/Nairobi)
GMT+03:00	Syowa Time (Antarctica/Syowa)
GMT+03:00	Arabian Standard Time (Asia/Aden)
GMT+03:00	Eastern European Standard Time (Asia/Amman)
GMT+03:00	Arabian Standard Time (Asia/Baghdad)
GMT+03:00	Arabian Standard Time (Asia/Bahrain)
GMT+03:00	Eastern European Standard Time (Asia/Damascus)
GMT+03:00	Arabian Standard Time (Asia/Kuwait)
GMT+03:00	Arabian Standard Time (Asia/Qatar)
GMT+03:00	Arabian Standard Time (Asia/Riyadh)
GMT+03:00	Eastern European Standard Time (Europe/Istanbul)
GMT+03:00	Moscow Standard Time (Europe/Kirov)
GMT+03:00	Moscow Standard Time (Europe/Minsk)
GMT+03:00	Moscow Standard Time (Europe/Moscow)
GMT+03:00	Moscow Standard Time (Europe/Simferopol)
GMT+03:00	Volgograd Standard Time (Europe/Volgograd)
GMT+03:00	East Africa Time (Indian/Antananarivo)
GMT+03:00	East Africa Time (Indian/Comoro)
GMT+03:00	East Africa Time (Indian/Mayotte)
GMT+02:00	Central Africa Time (Africa/Blantyre)
GMT+02:00	Central Africa Time (Africa/Bujumbura)
GMT+02:00	Eastern European Standard Time (Africa/Cairo)
GMT+03:00	Eastern European Standard Time (Africa/Cairo)
GMT+02:00	Central Africa Time (Africa/Gaborone)
GMT+02:00	Central Africa Time (Africa/Harare)
GMT+02:00	South Africa Standard Time (Africa/Johannesburg)
GMT+02:00	Central Africa Time (Africa/Juba)
GMT+02:00	Central Africa Time (Africa/Khartoum)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT+02:00	Central Africa Time (Africa/Kigali)
GMT+02:00	Central Africa Time (Africa/Lubumbashi)
GMT+02:00	Central Africa Time (Africa/Lusaka)
GMT+02:00	Central Africa Time (Africa/Maputo)
GMT+02:00	South Africa Standard Time (Africa/Maseru)
GMT+02:00	South Africa Standard Time (Africa/Mbabane)
GMT+02:00	Eastern European Standard Time (Africa/Tripoli)
GMT+02:00	Central Africa Time (Africa/Windhoek)
GMT+02:00	Eastern European Standard Time (Asia/Beirut)
GMT+03:00	Eastern European Summer Time (Asia/Beirut)
GMT+02:00	Eastern European Standard Time (Asia/Famagusta)
GMT+03:00	Eastern European Summer Time (Asia/Famagusta)
GMT+02:00	Eastern European Standard Time (Asia/Gaza)
GMT+03:00	Eastern European Summer Time (Asia/Gaza)
GMT+02:00	Eastern European Standard Time (Asia/Hebron)
GMT+03:00	Eastern European Summer Time (Asia/Hebron)
GMT+02:00	Israel Standard Time (Asia/Jerusalem)
GMT+03:00	Israel Daylight Time (Asia/Jerusalem)
GMT+02:00	Eastern European Standard Time (Asia/Nicosia)
GMT+03:00	Eastern European Summer Time (Asia/Nicosia)
GMT+02:00	Eastern European Standard Time (Europe/Athens)
GMT+03:00	Eastern European Summer Time (Europe/Athens)
GMT+02:00	Eastern European Standard Time (Europe/Bucharest)
GMT+03:00	Eastern European Summer Time (Europe/Bucharest)
GMT+02:00	Eastern European Standard Time (Europe/Chisinau)
GMT+03:00	Eastern European Summer Time (Europe/Chisinau)
GMT+02:00	Eastern European Standard Time (Europe/Helsinki)
GMT+03:00	Eastern European Summer Time (Europe/Helsinki)
GMT+02:00	Eastern European Standard Time (Europe/Kaliningrad)
GMT+02:00	Eastern European Standard Time (Europe/Kyiv)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT+03:00	Eastern European Summer Time (Europe/Kyiv)
GMT+02:00	Eastern European Standard Time (Europe/Mariehamn)
GMT+03:00	Eastern European Summer Time (Europe/Mariehamn)
GMT+02:00	Eastern European Standard Time (Europe/Riga)
GMT+03:00	Eastern European Summer Time (Europe/Riga)
GMT+02:00	Eastern European Standard Time (Europe/Sofia)
GMT+03:00	Eastern European Summer Time (Europe/Sofia)
GMT+02:00	Eastern European Standard Time (Europe/Tallinn)
GMT+03:00	Eastern European Summer Time (Europe/Tallinn)
GMT+02:00	Eastern European Standard Time (Europe/Uzhgorod)
GMT+03:00	Eastern European Summer Time (Europe/Uzhgorod)
GMT+02:00	Eastern European Standard Time (Europe/Vilnius)
GMT+03:00	Eastern European Summer Time (Europe/Vilnius)
GMT+02:00	Eastern European Standard Time (Europe/Zaporozhye)
GMT+03:00	Eastern European Summer Time (Europe/Zaporozhye)
GMT+01:00	Central European Standard Time (Africa/Algiers)
GMT+01:00	West Africa Standard Time (Africa/Bangui)
GMT+01:00	West Africa Standard Time (Africa/Brazzaville)
GMT+01:00	Central European Standard Time (Africa/Ceuta)
GMT+02:00	Central European Summer Time (Africa/Ceuta)
GMT+01:00	West Africa Standard Time (Africa/Douala)
GMT+01:00	West Africa Standard Time (Africa/Kinshasa)
GMT+01:00	West Africa Standard Time (Africa/Lagos)
GMT+01:00	West Africa Standard Time (Africa/Libreville)
GMT+01:00	West Africa Standard Time (Africa/Luanda)
GMT+01:00	West Africa Standard Time (Africa/Malabo)
GMT+01:00	West Africa Standard Time (Africa/Ndjamena)
GMT+01:00	West Africa Standard Time (Africa/Niamey)
GMT+01:00	West Africa Standard Time (Africa/Porto-Novo)
GMT+01:00	Central European Standard Time (Africa/Tunis)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT+01:00	Central European Standard Time (Arctic/Longyearbyen)
GMT+02:00	Central European Summer Time (Arctic/Longyearbyen)
GMT+01:00	Central European Standard Time (Europe/Amsterdam)
GMT+02:00	Central European Summer Time (Europe/Amsterdam)
GMT+01:00	Central European Standard Time (Europe/Andorra)
GMT+02:00	Central European Summer Time (Europe/Andorra)
GMT+01:00	Central European Standard Time (Europe/Belgrade)
GMT+02:00	Central European Summer Time (Europe/Belgrade)
GMT+01:00	Central European Standard Time (Europe/Berlin)
GMT+02:00	Central European Summer Time (Europe/Berlin)
GMT+01:00	Central European Standard Time (Europe/Bratislava)
GMT+02:00	Central European Summer Time (Europe/Bratislava)
GMT+01:00	Central European Standard Time (Europe/Brussels)
GMT+02:00	Central European Summer Time (Europe/Brussels)
GMT+01:00	Central European Standard Time (Europe/Budapest)
GMT+02:00	Central European Summer Time (Europe/Budapest)
GMT+01:00	Central European Standard Time (Europe/Busingen)
GMT+02:00	Central European Summer Time (Europe/Busingen)
GMT+01:00	Central European Standard Time (Europe/Copenhagen)
GMT+02:00	Central European Summer Time (Europe/Copenhagen)
GMT+01:00	Central European Standard Time (Europe/Gibraltar)
GMT+02:00	Central European Summer Time (Europe/Gibraltar)
GMT+01:00	Central European Standard Time (Europe/Ljubljana)
GMT+02:00	Central European Summer Time (Europe/Ljubljana)
GMT+01:00	Central European Standard Time (Europe/Luxembourg)
GMT+02:00	Central European Summer Time (Europe/Luxembourg)
GMT+01:00	Central European Standard Time (Europe/Madrid)
GMT+02:00	Central European Summer Time (Europe/Madrid)
GMT+01:00	Central European Standard Time (Europe/Malta)
GMT+02:00	Central European Summer Time (Europe/Malta)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT+01:00	Central European Standard Time (Europe/Monaco)
GMT+02:00	Central European Summer Time (Europe/Monaco)
GMT+01:00	Central European Standard Time (Europe/Oslo)
GMT+02:00	Central European Summer Time (Europe/Oslo)
GMT+01:00	Central European Standard Time (Europe/Paris)
GMT+02:00	Central European Summer Time (Europe/Paris)
GMT+01:00	Central European Standard Time (Europe/Podgorica)
GMT+02:00	Central European Summer Time (Europe/Podgorica)
GMT+01:00	Central European Standard Time (Europe/Prague)
GMT+02:00	Central European Summer Time (Europe/Prague)
GMT+01:00	Central European Standard Time (Europe/Rome)
GMT+02:00	Central European Summer Time (Europe/Rome)
GMT+01:00	Central European Standard Time (Europe/San_Marino)
GMT+02:00	Central European Summer Time (Europe/San_Marino)
GMT+01:00	Central European Standard Time (Europe/Sarajevo)
GMT+02:00	Central European Summer Time (Europe/Sarajevo)
GMT+01:00	Central European Standard Time (Europe/Skopje)
GMT+02:00	Central European Summer Time (Europe/Skopje)
GMT+01:00	Central European Standard Time (Europe/Stockholm)
GMT+02:00	Central European Summer Time (Europe/Stockholm)
GMT+01:00	Central European Standard Time (Europe/Tirane)
GMT+02:00	Central European Summer Time (Europe/Tirane)
GMT+01:00	Central European Standard Time (Europe/Vaduz)
GMT+02:00	Central European Summer Time (Europe/Vaduz)
GMT+01:00	Central European Standard Time (Europe/Vatican)
GMT+02:00	Central European Summer Time (Europe/Vatican)
GMT+01:00	Central European Standard Time (Europe/Vienna)
GMT+02:00	Central European Summer Time (Europe/Vienna)
GMT+01:00	Central European Standard Time (Europe/Warsaw)
GMT+02:00	Central European Summer Time (Europe/Warsaw)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT+01:00	Central European Standard Time (Europe/Zagreb)
GMT+02:00	Central European Summer Time (Europe/Zagreb)
GMT+01:00	Central European Standard Time (Europe/Zurich)
GMT+02:00	Central European Summer Time (Europe/Zurich)
GMT+00:00	Greenwich Mean Time (Africa/Abidjan)
GMT+00:00	Greenwich Mean Time (Africa/Accra)
GMT+00:00	Greenwich Mean Time (Africa/Bamako)
GMT+00:00	Greenwich Mean Time (Africa/Banjul)
GMT+00:00	Greenwich Mean Time (Africa/Bissau)
GMT+00:00	Western European Standard Time (Africa/Casablanca)
GMT+01:00	Western European Summer Time (Africa/Casablanca)
GMT+00:00	Greenwich Mean Time (Africa/Conakry)
GMT+00:00	Greenwich Mean Time (Africa/Dakar)
GMT+00:00	Western European Standard Time (Africa/El_Aaiun)
GMT+01:00	Western European Summer Time (Africa/El_Aaiun)
GMT+00:00	Greenwich Mean Time (Africa/Freetown)
GMT+00:00	Greenwich Mean Time (Africa/Lome)
GMT+00:00	Greenwich Mean Time (Africa/Monrovia)
GMT+00:00	Greenwich Mean Time (Africa/Nouakchott)
GMT+00:00	Greenwich Mean Time (Africa/Ouagadougou)
GMT+00:00	Greenwich Mean Time (Africa/Sao_Tome)
GMT+00:00	Greenwich Mean Time (America/Danmarkshavn)
GMT+00:00	Greenwich Mean Time (Antarctica/Troll)
GMT+02:00	Central European Summer Time (Antarctica/Troll)
GMT+00:00	Western European Standard Time (Atlantic/Canary)
GMT+01:00	Western European Summer Time (Atlantic/Canary)
GMT+00:00	Western European Standard Time (Atlantic/Faeroe)
GMT+01:00	Western European Summer Time (Atlantic/Faeroe)
GMT+00:00	Western European Standard Time (Atlantic/Madeira)
GMT+01:00	Western European Summer Time (Atlantic/Madeira)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT+00:00	Greenwich Mean Time (Atlantic/Reykjavik)
GMT+00:00	Greenwich Mean Time (Atlantic/St_Helena)
GMT+00:00	Greenwich Mean Time (Europe/Dublin)
GMT+01:00	Irish Standard Time (Europe/Dublin)
GMT+00:00	Greenwich Mean Time (Europe/Guernsey)
GMT+01:00	British Summer Time (Europe/Guernsey)
GMT+00:00	Greenwich Mean Time (Europe/Isle_of_Man)
GMT+01:00	British Summer Time (Europe/Isle_of_Man)
GMT+00:00	Greenwich Mean Time (Europe/Jersey)
GMT+01:00	British Summer Time (Europe/Jersey)
GMT+00:00	Western European Standard Time (Europe/Lisbon)
GMT+01:00	Western European Summer Time (Europe/Lisbon)
GMT+00:00	Greenwich Mean Time (Europe/London)
GMT+01:00	British Summer Time (Europe/London)
GMT+00:00	Greenwich Mean Time (GMT)
GMT-01:00	East Greenland Standard Time (America/Scoresbysund)
GMT+00:00	East Greenland Summer Time (America/Scoresbysund)
GMT-01:00	Azores Standard Time (Atlantic/Azores)
GMT+00:00	Azores Summer Time (Atlantic/Azores)
GMT-01:00	Cape Verde Standard Time (Atlantic/Cape_Verde)
GMT-02:00	Fernando de Noronha Standard Time (America/Noronha)
GMT-02:00	South Georgia Time (Atlantic/South_Georgia)
GMT-03:00	Brasilia Standard Time (America/Araguaina)
GMT-03:00	Argentina Standard Time (America/Argentina/Buenos_Aires)
GMT-03:00	Argentina Standard Time (America/Argentina/La_Rioja)
GMT-03:00	Argentina Standard Time (America/Argentina/Rio_Gallegos)
GMT-03:00	Argentina Standard Time (America/Argentina/Salta)
GMT-03:00	Argentina Standard Time (America/Argentina/San_Juan)
GMT-03:00	Argentina Standard Time (America/Argentina/San_Luis)
GMT-03:00	Argentina Standard Time (America/Argentina/Tucuman)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT-03:00	Argentina Standard Time (America/Argentina/Ushuaia)
GMT-03:00	Brasilia Standard Time (America/Bahia)
GMT-03:00	Brasilia Standard Time (America/Belem)
GMT-03:00	Argentina Standard Time (America/Catamarca)
GMT-03:00	French Guiana Time (America/Cayenne)
GMT-03:00	Argentina Standard Time (America/Cordoba)
GMT-03:00	Brasilia Standard Time (America/Fortaleza)
GMT-03:00	West Greenland Standard Time (America/Godthab)
GMT-02:00	West Greenland Summer Time (America/Godthab)
GMT-03:00	Argentina Standard Time (America/Jujuy)
GMT-03:00	Brasilia Standard Time (America/Maceio)
GMT-03:00	Argentina Standard Time (America/Mendoza)
GMT-03:00	St Pierre & Miquelon Standard Time (America/Miquelon)
GMT-02:00	St Pierre & Miquelon Daylight Time (America/Miquelon)
GMT-03:00	Uruguay Standard Time (America/Montevideo)
GMT-03:00	Suriname Time (America/Paramaribo)
GMT-03:00	Chile Standard Time (America/Punta_Arenas)
GMT-03:00	Brasilia Standard Time (America/Recife)
GMT-03:00	Brasilia Standard Time (America/Santarem)
GMT-03:00	Brasilia Standard Time (America/Sao_Paulo)
GMT-03:00	Chile Standard Time (Antarctica/Palmer)
GMT-03:00	Rothera Time (Antarctica/Rothera)
GMT-03:00	Falkland Islands Standard Time (Atlantic/Stanley)
GMT-03:30	Newfoundland Standard Time (America/St_Johns)
GMT-02:30	Newfoundland Daylight Time (America/St_Johns)
GMT-04:00	Atlantic Standard Time (America/Anguilla)
GMT-04:00	Atlantic Standard Time (America/Antigua)
GMT-04:00	Atlantic Standard Time (America/Aruba)
GMT-04:00	Paraguay Standard Time (America/Asuncion)
GMT-03:00	Paraguay Summer Time (America/Asuncion)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT-04:00	Atlantic Standard Time (America/Barbados)
GMT-04:00	Atlantic Standard Time (America/Blanc-Sablon)
GMT-04:00	Amazon Standard Time (America/Boa_Vista)
GMT-04:00	Amazon Standard Time (America/Campo_Grande)
GMT-04:00	Venezuela Time (America/Caracas)
GMT-04:00	Amazon Standard Time (America/Cuiaba)
GMT-04:00	Atlantic Standard Time (America/Curacao)
GMT-04:00	Atlantic Standard Time (America/Dominica)
GMT-04:00	Atlantic Standard Time (America/Glace_Bay)
GMT-03:00	Atlantic Daylight Time (America/Glace_Bay)
GMT-04:00	Atlantic Standard Time (America/Goose_Bay)
GMT-03:00	Atlantic Daylight Time (America/Goose_Bay)
GMT-04:00	Atlantic Standard Time (America/Grenada)
GMT-04:00	Atlantic Standard Time (America/Guadeloupe)
GMT-04:00	Guyana Time (America/Guyana)
GMT-04:00	Atlantic Standard Time (America/Halifax)
GMT-03:00	Atlantic Daylight Time (America/Halifax)
GMT-04:00	Atlantic Standard Time (America/Kralendijk)
GMT-04:00	Bolivia Time (America/La_Paz)
GMT-04:00	Atlantic Standard Time (America/Lower_Princes)
GMT-04:00	Amazon Standard Time (America/Manaus)
GMT-04:00	Atlantic Standard Time (America/Marigot)
GMT-04:00	Atlantic Standard Time (America/Martinique)
GMT-04:00	Atlantic Standard Time (America/Moncton)
GMT-03:00	Atlantic Daylight Time (America/Moncton)
GMT-04:00	Atlantic Standard Time (America/Montserrat)
GMT-04:00	Atlantic Standard Time (America/Port_of_Spain)
GMT-04:00	Amazon Standard Time (America/Porto_Velho)
GMT-04:00	Atlantic Standard Time (America/Puerto_Rico)
GMT-04:00	Chile Standard Time (America/Santiago)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT-03:00	Chile Summer Time (America/Santiago)
GMT-04:00	Atlantic Standard Time (America/Santo_Domingo)
GMT-04:00	Atlantic Standard Time (America/St_Barthelemy)
GMT-04:00	Atlantic Standard Time (America/St_Kitts)
GMT-04:00	Atlantic Standard Time (America/St_Lucia)
GMT-04:00	Atlantic Standard Time (America/St_Thomas)
GMT-04:00	Atlantic Standard Time (America/St_Vincent)
GMT-04:00	Atlantic Standard Time (America/Thule)
GMT-03:00	Atlantic Daylight Time (America/Thule)
GMT-04:00	Atlantic Standard Time (America/Tortola)
GMT-04:00	Atlantic Standard Time (Atlantic/Bermuda)
GMT-03:00	Atlantic Daylight Time (Atlantic/Bermuda)
GMT-05:00	Colombia Standard Time (America/Bogota)
GMT-05:00	Eastern Standard Time (America/Cancun)
GMT-05:00	Eastern Standard Time (America/Cayman)
GMT-05:00	Eastern Standard Time (America/Coral_Harbour)
GMT-05:00	Eastern Standard Time (America/Detroit)
GMT-04:00	Eastern Daylight Time (America/Detroit)
GMT-05:00	Acre Standard Time (America/Eirunepe)
GMT-05:00	Eastern Standard Time (America/Grand_Turk)
GMT-04:00	Eastern Daylight Time (America/Grand_Turk)
GMT-05:00	Ecuador Time (America/Guayaquil)
GMT-05:00	Cuba Standard Time (America/Havana)
GMT-04:00	Cuba Daylight Time (America/Havana)
GMT-05:00	Eastern Standard Time (America/Indiana/Indianapolis)
GMT-04:00	Eastern Daylight Time (America/Indiana/Indianapolis)
GMT-05:00	Eastern Standard Time (America/Indiana/Marengo)
GMT-04:00	Eastern Daylight Time (America/Indiana/Marengo)
GMT-05:00	Eastern Standard Time (America/Indiana/Petersburg)
GMT-04:00	Eastern Daylight Time (America/Indiana/Petersburg)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT-05:00	Eastern Standard Time (America/Indiana/Vevay)
GMT-04:00	Eastern Daylight Time (America/Indiana/Vevay)
GMT-05:00	Eastern Standard Time (America/Indiana/Vincennes)
GMT-04:00	Eastern Daylight Time (America/Indiana/Vincennes)
GMT-05:00	Eastern Standard Time (America/Indiana/Winamac)
GMT-04:00	Eastern Daylight Time (America/Indiana/Winamac)
GMT-05:00	Eastern Standard Time (America/Iqaluit)
GMT-04:00	Eastern Daylight Time (America/Iqaluit)
GMT-05:00	Eastern Standard Time (America/Jamaica)
GMT-05:00	Eastern Standard Time (America/Kentucky/Monticello)
GMT-04:00	Eastern Daylight Time (America/Kentucky/Monticello)
GMT-05:00	Peru Standard Time (America/Lima)
GMT-05:00	Eastern Standard Time (America/Louisville)
GMT-04:00	Eastern Daylight Time (America/Louisville)
GMT-05:00	Eastern Standard Time (America/Montreal)
GMT-04:00	Eastern Daylight Time (America/Montreal)
GMT-05:00	Eastern Standard Time (America/Nassau)
GMT-04:00	Eastern Daylight Time (America/Nassau)
GMT-05:00	Eastern Standard Time (America/New_York)
GMT-04:00	Eastern Daylight Time (America/New_York)
GMT-05:00	Eastern Standard Time (America/Nipigon)
GMT-04:00	Eastern Daylight Time (America/Nipigon)
GMT-05:00	Eastern Standard Time (America/Panama)
GMT-05:00	Eastern Standard Time (America/Pangnirtung)
GMT-04:00	Eastern Daylight Time (America/Pangnirtung)
GMT-05:00	Eastern Standard Time (America/Port-au-Prince)
GMT-04:00	Eastern Daylight Time (America/Port-au-Prince)
GMT-05:00	Acre Standard Time (America/Rio_Branco)
GMT-05:00	Eastern Standard Time (America/Thunder_Bay)
GMT-04:00	Eastern Daylight Time (America/Thunder_Bay)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT-05:00	Eastern Standard Time (America/Toronto)
GMT-04:00	Eastern Daylight Time (America/Toronto)
GMT-06:00	Central Standard Time (America/Bahia_Banderas)
GMT-06:00	Central Standard Time (America/Belize)
GMT-06:00	Central Standard Time (America/Chicago)
GMT-05:00	Central Daylight Time (America/Chicago)
GMT-06:00	Mexican Pacific Standard Time (America/Chihuahua)
GMT-06:00	Central Standard Time (America/Costa_Rica)
GMT-06:00	Central Standard Time (America/El_Salvador)
GMT-06:00	Central Standard Time (America/Guatemala)
GMT-06:00	Central Standard Time (America/Indiana/Knox)
GMT-05:00	Central Daylight Time (America/Indiana/Knox)
GMT-06:00	Central Standard Time (America/Indiana/Tell_City)
GMT-05:00	Central Daylight Time (America/Indiana/Tell_City)
GMT-06:00	Central Standard Time (America/Managua)
GMT-06:00	Central Standard Time (America/Matamoros)
GMT-05:00	Central Daylight Time (America/Matamoros)
GMT-06:00	Central Standard Time (America/Menominee)
GMT-05:00	Central Daylight Time (America/Menominee)
GMT-06:00	Central Standard Time (America/Merida)
GMT-06:00	Central Standard Time (America/Mexico_City)
GMT-06:00	Central Standard Time (America/Monterrey)
GMT-06:00	Central Standard Time (America/North_Dakota/Beulah)
GMT-05:00	Central Daylight Time (America/North_Dakota/Beulah)
GMT-06:00	Central Standard Time (America/North_Dakota/Center)
GMT-05:00	Central Daylight Time (America/North_Dakota/Center)
GMT-06:00	Central Standard Time (America/North_Dakota/New_Salem)
GMT-05:00	Central Daylight Time (America/North_Dakota/New_Salem)
GMT-06:00	Mountain Standard Time (America/Ojinaga)
GMT-05:00	Mountain Daylight Time (America/Ojinaga)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT-06:00	Central Standard Time (America/Rainy_River)
GMT-05:00	Central Daylight Time (America/Rainy_River)
GMT-06:00	Central Standard Time (America/Rankin_Inlet)
GMT-05:00	Central Daylight Time (America/Rankin_Inlet)
GMT-06:00	Central Standard Time (America/Regina)
GMT-06:00	Central Standard Time (America/Resolute)
GMT-05:00	Central Daylight Time (America/Resolute)
GMT-06:00	Central Standard Time (America/Swift_Current)
GMT-06:00	Central Standard Time (America/Tegucigalpa)
GMT-06:00	Central Standard Time (America/Winnipeg)
GMT-05:00	Central Daylight Time (America/Winnipeg)
GMT-06:00	Easter Island Standard Time (Pacific/Easter)
GMT-05:00	Easter Island Summer Time (Pacific/Easter)
GMT-06:00	Galapagos Time (Pacific/Galapagos)
GMT-07:00	Mountain Standard Time (America/Boise)
GMT-06:00	Mountain Daylight Time (America/Boise)
GMT-07:00	Mountain Standard Time (America/Cambridge_Bay)
GMT-06:00	Mountain Daylight Time (America/Cambridge_Bay)
GMT-07:00	Mountain Standard Time (America/Creston)
GMT-07:00	Yukon Time (America/Dawson)
GMT-07:00	Mountain Standard Time (America/Dawson_Creek)
GMT-07:00	Mountain Standard Time (America/Denver)
GMT-06:00	Mountain Daylight Time (America/Denver)
GMT-07:00	Mountain Standard Time (America/Edmonton)
GMT-06:00	Mountain Daylight Time (America/Edmonton)
GMT-07:00	Mountain Standard Time (America/Fort_Nelson)
GMT-07:00	Mexican Pacific Standard Time (America/Hermosillo)
GMT-07:00	Mountain Standard Time (America/Inuvik)
GMT-06:00	Mountain Daylight Time (America/Inuvik)
GMT-07:00	Mexican Pacific Standard Time (America/Mazatlan)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT-07:00	Mountain Standard Time (America/Phoenix)
GMT-07:00	Yukon Time (America/Whitehorse)
GMT-07:00	Mountain Standard Time (America/Yellowknife)
GMT-06:00	Mountain Daylight Time (America/Yellowknife)
GMT-08:00	Pacific Standard Time (America/Los_Angeles)
GMT-07:00	Pacific Daylight Time (America/Los_Angeles)
GMT-08:00	Northwest Mexico Standard Time (America/Santa_Isabel)
GMT-07:00	Northwest Mexico Daylight Time (America/Santa_Isabel)
GMT-08:00	Pacific Standard Time (America/Tijuana)
GMT-07:00	Pacific Daylight Time (America/Tijuana)
GMT-08:00	Pacific Standard Time (America/Vancouver)
GMT-07:00	Pacific Daylight Time (America/Vancouver)
GMT-08:00	Pitcairn Time (Pacific/Pitcairn)
GMT-09:00	Alaska Standard Time (America/Anchorage)
GMT-08:00	Alaska Daylight Time (America/Anchorage)
GMT-09:00	Alaska Standard Time (America/Juneau)
GMT-08:00	Alaska Daylight Time (America/Juneau)
GMT-09:00	Alaska Standard Time (America/Metlakatla)
GMT-08:00	Alaska Daylight Time (America/Metlakatla)
GMT-09:00	Alaska Standard Time (America/Nome)
GMT-08:00	Alaska Daylight Time (America/Nome)
GMT-09:00	Alaska Standard Time (America/Sitka)
GMT-08:00	Alaska Daylight Time (America/Sitka)
GMT-09:00	Alaska Standard Time (America/Yakutat)
GMT-08:00	Alaska Daylight Time (America/Yakutat)
GMT-09:00	Gambier Time (Pacific/Gambier)
GMT-09:30	Marquesas Time (Pacific/Marquesas)
GMT-10:00	Hawaii-Aleutian Standard Time (America/Adak)
GMT-09:00	Hawaii-Aleutian Daylight Time (America/Adak)
GMT-10:00	Hawaii-Aleutian Standard Time (Pacific/Honolulu)

TIME_ZONE_CODE	TIME_ZONE_NAME
GMT-10:00	Hawaii-Aleutian Standard Time (Pacific/Johnston)
GMT-10:00	Cook Islands Standard Time (Pacific/Rarotonga)
GMT-10:00	Tahiti Time (Pacific/Tahiti)
GMT-11:00	Samoa Standard Time (Pacific/Midway)
GMT-11:00	Niue Time (Pacific/Niue)
GMT-11:00	Samoa Standard Time (Pacific/Pago_Pago)

Synchronize Local System Clocks with UTC Time

If needed, you can synchronize your local system clocks with the UTC time.

If your local clocks are deployed on Amazon Web Services, you can use Network Time Protocol (NTP) sources as described in [Keeping Time With Amazon Time Sync Service](#).

If your local clocks are deployed outside of Amazon Web Services, you can use one of the NIST Internet Time Servers as described in [NIST Internet Time Service \(ITS\)](#).

SEE ALSO:

[Language, Locale, and Currency Settings](#)

Local Name Fields

Local name fields are additional standard text fields that allow you to define original or translated text for certain fields on Account, Contact, and Lead objects. For example, you can define local name fields for a contact so that their name appears in a language appropriate for their locale.

Your users can use local name fields in addition to the other name fields to filter, search for, and categorize records, and to build reports. Local name fields are included in search results.

The following local name fields are available for the Account, Contact, and Lead objects.

Object	Local Name Field
Account	Account Name (local)
Contact	First Name (local)
Contact	Last Name (local)
Lead	Company Name (local)
Lead	First Name (local)
Lead	Last Name (local)

For example, you can define local name fields for a contact in Japan named Yukiko Nakamura:

EDITIONS

Available in: both Lightning Experience and Salesforce Classic ([not available in all orgs](#)).

Available in: **All Editions** except **Database.com**

Field	Value
First Name	Yukiko
First Name (Local)	
Last Name	Nakamura
Last Name (Local)	

 **Note:** When viewed from a report, empty local name fields display different values depending on whether the report is standard or custom. If the local name field is empty:

- Standard reports display the value from the standard name field. So if `First Name (Local)` is empty, the value for `First Name` is displayed.
- Custom reports display an empty value. So if `First Name (Local)` is empty, the field is displayed empty.

Enable Local Name Fields

If you don't see local name fields for accounts, contacts, and leads in your org, have your system administrator log a case with Salesforce Support. Include the following information:

- A business reason for the request
- Your organization ID

Then add your desired local name fields to page layouts and make them visible to appropriate user profiles.

[Add Local Name Fields to a Page Layout in Salesforce Classic](#)

By default, local name fields don't appear in page layouts for accounts, contacts, or leads. To see a local name field on one of these pages, add it to the page layout and then make it visible using Field-Level Security settings.

[Add Local Name Fields to a Page Layout in Lightning Experience](#)

By default, local name fields don't appear in page layouts for accounts, contacts, or leads. To see a local name field on one of these pages, add it to the page layout and then make it visible using Field-Level Security settings.

Add Local Name Fields to a Page Layout in Salesforce Classic

By default, local name fields don't appear in page layouts for accounts, contacts, or leads. To see a local name field on one of these pages, add it to the page layout and then make it visible using Field-Level Security settings.

1. From Setup, select **Customize**.
2. Select the object with the local name field.
3. Select **Page Layout** and click **Edit**.
4. Drag the local name field to the record section.
5. Click **Save**.
6. From Setup, select **Security Controls** and then select **Field Accessibility**.
7. Select the object with the local name field.
8. Select **View By Fields**.
9. Select the local name field and make it visible to your desired profiles.

10. Click **Save**.

Add Local Name Fields to a Page Layout in Lightning Experience

By default, local name fields don't appear in page layouts for accounts, contacts, or leads. To see a local name field on one of these pages, add it to the page layout and then make it visible using Field-Level Security settings.

1. From Setup, select **Object Manager**.
2. Select the object with the local name field.
3. Select **Page Layout** and click the page layout to edit it.
4. Drag the local name field to the record section.
5. Click **Save**.
6. From Setup, select **Home**, then **Security**, and then select **Field Accessibility**.
7. Select the object with the local name field.
8. Select **View By Fields**.
9. Select the local name field and make it visible to your desired profiles.
10. Click **Save**.

Enable the Japanese Imperial Calendar

Display the imperial calendar for users with the Japanese (Japan) locale.

1. From Setup, enter `user` in the Quick Find box.
2. Select **User Interface**.
3. Select **Enable Japanese Imperial Calendar in Lightning Experience for the Japanese (Japan) locale**.

 **Example:** When the imperial calendar is enabled, only users with a locale of “Japanese (Japan)” can see it (1).



The imperial calendar information is hidden for users with other locales (2).

Make sure that users who want to view the imperial calendar set their locale to Japanese (Japan) and their language to Japanese.

EDITIONS

Available in: Lightning Experience

Available in: **Group, Professional, Enterprise, Performance, Unlimited,** and **Database.com** Editions

USER PERMISSIONS

To modify user interface settings:

- Customize Application

Define Your Fiscal Year

Specify a fiscal year that fits your business needs.

If your fiscal year follows the Gregorian calendar, but does not start in January, you can define a standard fiscal year with a different starting month. If your fiscal year follows a different structure from the Gregorian calendar, you can define a custom fiscal year that meets your needs.

Whether you use a standard fiscal year or a custom fiscal year, you define individual fiscal years one time. These fiscal year definitions allow you to use these fiscal periods throughout Salesforce including in reporting, opportunities, and forecasting.

 **Tip:** As a best practice, update product schedules whenever a custom fiscal year is created or changed.

Standard Fiscal Years

Standard fiscal years follow the Gregorian calendar, but can start on the first day of any month of the year.

Custom Fiscal Years

Some companies break down their fiscal years, quarters, and weeks into custom fiscal periods based on their financial planning requirements. Salesforce allows you to flexibly define these periods using custom fiscal years. For example, you can create a 13-week quarter represented by three periods of four, four, and five weeks, rather than calendar months.

If you use a common fiscal year structure, such as 4-4-5 or a 13-period structure, you can rapidly define a fiscal year. Just specify a start date and choose an included template. If the fiscal year structure you need is not among the templates, you can easily modify a template to suit your business. For example, if you use three fiscal quarters per year (a trimester) rather than four, delete or modify quarters and periods to meet your needs.

Your custom fiscal periods can be named based on your standards. For example, a fiscal period could be called “P2” or “February.”

Fiscal years can be modified any time. For example, you can add an extra week to synchronize a custom fiscal year with a standard calendar in a leap year. Changes to fiscal year structure take effect immediately upon being saved. If you use forecasting, Salesforce recalculates your forecasts when you save changes to a fiscal year.

Considerations for Enabling Custom Fiscal Years

Before enabling custom fiscal years, consider these key points.

- After you enable custom fiscal years, you can't disable the feature. However, to revert to standard fiscal years, you can define custom fiscal years that follow the same Gregorian calendar structure as the Salesforce standard fiscal years.
- Fiscal year definitions are not automatically created. Define a custom fiscal year for each year you do business.
- Enabling or defining custom fiscal years impacts your forecasts, reports, and quotas.
 - When you define the first custom fiscal year, all existing forecasts, forecast history, and forecast adjustments from the year's first period forward are deleted. Forecasts for periods before the first custom fiscal year are not deleted and can be accessed as usual.
 - When you define a new custom fiscal year, any existing forecasts, forecast history, forecast adjustments, and quotas for the corresponding standard fiscal year are lost.
- You can't use fiscal period columns in opportunity, opportunity with product, or opportunity with schedule reports.
- Opportunity list views don't include a fiscal period column.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions** except for **Database.com**.

USER PERMISSIONS

To define or edit fiscal years:

- Customize Application

- When custom fiscal years are enabled, you can't use the `FISCAL_MONTH()`, `FISCAL_QUARTER()`, or `FISCAL_YEAR()` date functions in SOQL.

Set the Fiscal Year

If your company follows the Gregorian calendar year but you want to change the fiscal year start month, use standard fiscal years. If your company does not observe a standard fiscal year, you can enable custom fiscal years, which define a more complex fiscal year structure.

Customize the Fiscal Year Structure

If your custom fiscal year needs a different structure than one available from the templates, modify the details of your custom fiscal year definition.

Customize the Fiscal Year Labels

Customize the labels of your fiscal years in two ways: Naming schemes and prefix choices or fiscal year picklist customization.

Choose a Custom Fiscal Year Template

When defining a new custom fiscal year, your first step is to choose a custom fiscal year template.

Define or Modify a Custom Fiscal Year

Set up your company's custom fiscal years to fit your company's calendar. If you define a custom fiscal year and want to change it, edit the existing fiscal year definition.

Set the Fiscal Year

If your company follows the Gregorian calendar year but you want to change the fiscal year start month, use standard fiscal years. If your company does not observe a standard fiscal year, you can enable custom fiscal years, which define a more complex fiscal year structure.

-  **Warning:** If you change your fiscal year start month, quota and adjustment information is purged.

For specific information on both types of fiscal years, see [Define Your Fiscal Year](#) on page 291.

1. Back up your current data and export it into a set of comma-separated values (CSV) files. Run a data backup export because changing the fiscal year causes fiscal periods to shift. This change affects opportunities and forecasts organization-wide.
2. From Setup, enter *Fiscal Year* in the **Quick Find** box, then select **Fiscal Year**.
3. Select **Standard Fiscal Year** or **Custom Fiscal Year**.
 - To create a standard fiscal year, choose the start month. Then specify whether the fiscal year name is based on the year in which it begins or ends.
 - To create a custom fiscal year, click **Enable Custom Fiscal Years**, click **OK**, and define your fiscal year.

Custom fiscal years cannot be disabled once enabled. Enabling custom fiscal years has impacts on your reports, forecasts, quotas, and other date-sensitive material. Do not enable custom fiscal years unless you understand and are prepared for all the implications.

4. Click **Save**.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions** except for **Database.com**.

USER PERMISSIONS

To change fiscal year:

- **Customize Application**

Customize the Fiscal Year Structure

If your custom fiscal year needs a different structure than one available from the templates, modify the details of your custom fiscal year definition.

 **Warning:** Changing the length of a fiscal year has an impact on forecasting and reporting. For detailed information on the impact, see [Define Your Fiscal Year](#).

If you want to return to a fiscal year template, select a template from the **Reset Fiscal Year Structure** drop-down list. However, resetting the fiscal year structure to a template removes all the customizations you made to the fiscal year.

You can easily add or remove fiscal periods (such as quarters, periods, or weeks) from the fiscal year structure.

1. From Setup, click **Company Profile > Fiscal Year**.
2. Click **Edit** for the fiscal year you want to edit.
3. If it is not already expanded, expand the **Advanced Customization** section.
4. At this point you can add and remove fiscal periods, and change the length of fiscal periods.
 - To add a new fiscal period, select the checkbox for the period before the new period, then click **Insert**.
For example, to add a quarter, and you want it to be the second quarter, select the checkbox for the first quarter. The maximum number of fiscal periods is 250.
 - To remove a fiscal period, select the checkbox for the period you want to delete, then click **Delete**.
You must have at least one quarter, one period, and one week. If you delete a fiscal period or quarter, you delete forecast adjustments and quotas for that period or quarter.
 - To change the length of a fiscal period, choose the length from the **Duration** drop-down list for the fiscal week.
To change the duration of a fiscal period or quarter, insert or delete weeks, or change the length of weeks that compose the period or quarter.
5. After you have customized your fiscal year, preview the fiscal year definition.
6. Save your work.

Customize the Fiscal Year Labels

Customize the labels of your fiscal years in two ways: Naming schemes and prefix choices or fiscal year picklist customization.

When defining a custom fiscal year, you can choose the labeling scheme to use for your custom fiscal year. Each fiscal period type (quarter, period, and week) has a list of labeling schemes that you can select.

Table 2: Fiscal Year Naming Schemes and Prefix Choices

Scheme	Option	Description
Quarter Name Scheme	Numbered by Year	This option allows you to add the quarter number to the quarter label. The quarter label is a combination of the label for the quarter prefix and the quarter number. For example, if the quarter prefix is "Q", the label for the third quarter Q3. By default the order of the quarter determines its number (the first quarter is labeled "1"). To customize the order, select a different value from the quarter detail drop-down list.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **All Editions** except for **Database.com**.

USER PERMISSIONS

To define or edit fiscal years:

- Customize Application

USER PERMISSIONS

To define or edit fiscal years:

- Customize Application

Scheme	Option	Description
	Customer Quarter Names	This option allows you to set the quarter label to any name. The quarter label is set to the name you select from <code>Quarter Name</code> . By default the order of the quarter names is the same as the picklist order. To customize the order, select a different value from the quarter detail drop-down list.
Period Name Scheme	Numbered By Year	This option allows you to set the period label based on its position in the year. The period label is a combination of the period prefix and the period number. Period numbers do not reset in each quarter. For example, if the period prefix is "P," the label for the sixth period is P6. By default the order of the period determines its number (the first period is labeled "1"). To customize the number, select a different value from the period detail drop-down list.
	Numbered By Quarter	This option allows you to set the period label based on its position in the quarter. The period label is a combination of the period prefix and the period number. Period numbers reset in each quarter. For example, if the period prefix is "P," and the sixth period is the second period in the second quarter, its label is P2. By default the number for each period is set by their order within the quarter (the first period in a quarter is labeled "1"); customize it by selecting a different value from the period detail drop-down list.
	Standard Month Names	This option allows you to set the period label to the month name of the start of the period. For example, if a period started on October 12 and ends on November 10, the period label would be October.
	Custom Period Names	This option allows you to set the period label to any string. The period label is set to the string you select from <code>Period Name</code> . By default the order of the period names is the same as the picklist order, which you can customize by selecting a different value from the period detail drop-down list.

Table 3: Fiscal Year Picklists

Picklist	Description
<code>Quarter Prefix</code>	The quarter prefix picklist is a list of options for the text that prefixes the quarter number or name if your fiscal year uses the Numbered By Year quarter naming scheme. For example, if the fiscal quarter is called "Q4," the "Q" is the quarter prefix.
<code>Period Prefix</code>	The period prefix picklist is a list of options for the text that prefixes the period number or name if your fiscal year uses the Numbered By Year period naming scheme. For example, if the fiscal quarter is called "P4," the "P" is the period prefix.
<code>Quarter Name</code>	The quarter name picklist is a list of options for the quarter name if your fiscal year uses the Custom Quarter Names quarter naming scheme. For example, if you want to name your quarters for the seasons (Spring, Summer, Fall, and Winter), you could set the quarter name list to those values.
<code>Period Name</code>	The period name picklist is a list of options for the quarter name if your fiscal year uses the Custom Period Names quarter naming scheme. Similar to the quarter name picklist, you can choose meaningful names for the period name picklist.

1. To customize a picklist, from Setup, click **Company Profile > Fiscal Year**.
2. Click **Edit** next to the appropriate picklist.

SEE ALSO:

[Define Your Fiscal Year](#)

Choose a Custom Fiscal Year Template

When defining a new custom fiscal year, your first step is to choose a custom fiscal year template.

These templates are available to make it easier for you to define your custom fiscal year. They create a simple custom fiscal year that you can customize to meet your exact needs.

 **Note:** If you choose a template and realize that it is not the best one for your fiscal year definition, you can reset it at any time using the **Reset Fiscal Year Structure** option.

Choose one of three types of templates:

- **4 Quarters per Year, 13 Weeks per Quarter**

Choose one of these templates for your fiscal year if you want each quarter to have the same number of weeks per quarter. These templates all have 4 quarters, 12 periods, and 52 weeks per year. Each quarter is 13 weeks long and is composed of three periods. Two of the periods in each quarter are 4 weeks, and one is 5 weeks. In a 4-4-5 template, for example, the first and second period of a quarter are 4 weeks long, and the third period is 5 weeks long. Weeks are always 7 days long. A typical customization for these templates is to add extra weeks for leap years.

4-4-5	Within each quarter, period 1 has 4 weeks, period 2 has 4 weeks, and period 3 has 5 weeks
4-5-4	Within each quarter, period 1 has 4 weeks, period 2 has 5 weeks, and period 3 has 4 weeks
5-4-4	Within each quarter, period 1 has 5 weeks, period 2 has 4 weeks, and period 3 has 4 weeks

- **13 Periods per Year, 4 Weeks per Period**

Choose one of these templates if your fiscal year has more than 12 periods and if one quarter is longer than the other quarters. These templates all have 4 quarters per year, 13 periods per year, 3 or 4 periods per quarter, 53 weeks per year, and 4 weeks per period (5 weeks in the final period). Weeks generally have 7 days, but include a short week at the end of a year. The most common customization for this type of template is to create or change the length of a short week.

3-3-3-4	Quarter 1 has 3 periods, quarter 2 has 3 periods, quarter 3 has 3 periods, and quarter 4 has 4 periods
3-3-4-3	Quarter 1 has 3 periods, quarter 2 has 3 periods, quarter 3 has 4 periods, and quarter 4 has 3 periods
3-4-3-3	Quarter 1 has 3 periods, quarter 2 has 4 periods, quarter 3 has 3 periods, and quarter 4 has 3 periods
4-3-3-3	Quarter 1 has 4 periods, quarter 2 has 3 periods, quarter 3 has 3 periods, and quarter 4 has 3 periods

- **Gregorian Calendar**

12 months/year, standard Gregorian calendar.

USER PERMISSIONS

To change your fiscal year:

- **Customize Application**

Unlike the other template styles, you can't do advanced customization of a fiscal year that has been created from a Gregorian calendar template. Only use this template if you want to create a fiscal year that follows the Gregorian calendar. This template mimics the functionality of standard fiscal years.

SEE ALSO:

[Define Your Fiscal Year](#)

Define or Modify a Custom Fiscal Year

Set up your company's custom fiscal years to fit your company's calendar. If you define a custom fiscal year and want to change it, edit the existing fiscal year definition.

Before defining a custom fiscal year, enable custom fiscal years. See [Set the Fiscal Year](#) on page 292 for more information.

Before defining or editing any custom fiscal years, be aware of its impact on forecasting, reports, and other objects by reviewing [Define Your Fiscal Year](#) on page 291.

If your company uses forecasting, creating the first custom fiscal year deletes any quotas and adjustments in the corresponding and subsequent standard fiscal years.

Custom fiscal years cannot be deleted.

1. To define a new custom fiscal year, navigate to Setup, click **Company Profile > Fiscal Year**
2. Click **New**. The Custom Fiscal Year template dialog opens.
3. Choose a template and click **Continue** to close the Custom Fiscal Year template dialog. For more information on the templates, see [Choose a Custom Fiscal Year Template](#) on page 295.
4. Set the fiscal year start date, the fiscal year name, and choose the week start day. You can also add a description for the fiscal year. For the first custom fiscal year, the `Fiscal Year Start Date` and the `Week Start Date` are automatically set to today's date and day of week. If you already defined a custom fiscal year, the start dates are set to the day after the last end date of your custom fiscal years. To change other than the start date, year name, or week start day, see [Customize the Fiscal Year Structure](#) on page 293.
5. To review the fiscal year definition, click **Preview**.
6. If it is correct, close the preview and click **Save** to save your fiscal year, or **Save & New** to save your fiscal year and define another fiscal year.

If you want to make changes to a previously defined custom fiscal year, click **Edit** for the fiscal year you want to edit. Change the `Fiscal Year Start Date`, the `Fiscal Year Name`, `Description`, or `Week Start Day`. Click **Preview** to review the fiscal year definition, then click **Save**.

Sometimes changing the `Fiscal Year Start Date` causes this fiscal year to overlap with the previous fiscal year or create a gap between the fiscal years. In this case, the end date of the previous fiscal year is changed to the day before the start of this fiscal year.

If changing the end date causes this fiscal year to overlap the next fiscal year, or create a gap between the fiscal years, the start date of the next fiscal year changes to the day after the end of this fiscal year. You can't change the start or end date of a fiscal year if that causes it to overlap with a fiscal year that is defined using a Gregorian year template.

To make more detailed edits, see [Customize the Fiscal Year Structure](#) on page 293.

The default label values for the fiscal year periods determine the fiscal year period labels for forecasting and reporting, unless you specify them. To change them, see [Customize the Fiscal Year Labels](#) on page 293.

USER PERMISSIONS

To change your fiscal year:

- [Customize Application](#)

 **Warning:** If you change the start or end date of any quarter, period, or week, you lose all forecast data that are within that date range, including quotas, forecast history, and forecast adjustments. It also includes all forecasts for date ranges automatically adjusted as a result of that change and end or start date changes resulting from inserting or deleting periods.

Einstein Terms and Data Usage

Some Einstein features require you to accept terms and review usage limitations before turning them on. Also, review which data is used for global models.

[Turn Einstein Features On or Off](#)

See if your Sales Cloud, Service Cloud, or Lightning Platform license comes with included Einstein features. Access to included Einstein features may be subject to usage limitations and your acceptance of additional terms.

[Einstein and Data Usage](#)

Einstein intelligence is built on data. As an Einstein customer, it is important for you to know what data is being used in your Einstein products. Tables here list the data usage for all features in Sales Cloud, Service Cloud, Lightning Platform, Commerce Cloud (B2C Commerce, B2B Commerce, and D2C Commerce), Marketing Cloud Account Engagement, and Marketing Cloud Growth.

Turn Einstein Features On or Off

See if your Sales Cloud, Service Cloud, or Lightning Platform license comes with included Einstein features. Access to included Einstein features may be subject to usage limitations and your acceptance of additional terms.

Setup and learn more about each feature in Help.

Cloud	Feature	Editions	Instructions
Sales	Einstein Activity Capture	Professional, Enterprise, Performance, and Unlimited	Set Up Einstein Activity Capture
Sales	Sales Cloud Einstein	Unlimited	Set Up Sales Cloud Einstein
Sales	Einstein Conversation Insights	Unlimited	Set Up Einstein Conversation Insights
Sales	Einstein Opportunity Scoring	Enterprise, Performance, and Unlimited	Enable Einstein Opportunity Scoring
Sales	Einstein Deal Insights	Enterprise, Performance, and Unlimited	Turn On Pipeline Inspection
Sales	Sales Engagement	Unlimited	Set Up Sales Engagement
Sales	Salesforce Inbox	Unlimited	Turn On Salesforce Inbox
Service	Einstein Article Recommendations	Enterprise, Performance, and Unlimited	Set Up Einstein Article Recommendations
Service	Einstein Bots	Unlimited	Enable Einstein Bots

Cloud	Feature	Editions	Instructions
Service	Einstein Case Classification	Enterprise, Performance, and Unlimited	Set Up Einstein Case Classification
Service	Einstein Case Wrap Up	Enterprise, Performance, and Unlimited	Set Up Einstein Case Wrap Up
Platform	Einstein Prediction Builder	Enterprise, Performance, Unlimited, and Developer	Turn Einstein Prediction Builder On or Off
Platform	Einstein Recommendation Builder	Enterprise, Performance, Unlimited, and Developer	Set Up Einstein Recommendation Builder

If you can't turn on these features without your System Administrator's permissions, see [Submitting an Order Form Supplement for Einstein Features](#) for instructions.

At this time, Einstein features aren't available on the Salesforce Government Cloud.

For more information on Einstein features, see the [Salesforce Trust and Compliance Documentation](#).

Einstein and Data Usage

Einstein intelligence is built on data. As an Einstein customer, it is important for you to know what data is being used in your Einstein products. Tables here list the data usage for all features in Sales Cloud, Service Cloud, Lightning Platform, Commerce Cloud (B2C Commerce, B2B Commerce, and D2C Commerce), Marketing Cloud Account Engagement, and Marketing Cloud Growth.

The tables list both the Customer Data, which is data submitted by the Customer to our services as defined in our [Main Services Agreement \(MSA\)](#), and the usage data, which is data relating to users interactions with Salesforce. Data submitted to an Einstein feature may be used to train AI models, to improve your services and features, or to develop new features that you will have access to without additional cost.

The tables also indicate which features use global models, which are models that look for aggregated, anonymous trends across multiple Salesforce Customers. The Customer has control over whether their data contributes to global models. For more information on how to control how your data is used, see [Salesforce Einstein: Global Model Opt-Out Process](#).

[Einstein and Data Usage in Sales Cloud, Service Cloud, Marketing Cloud Account Engagement, Marketing Cloud Growth, and Lightning Platform](#)

As an Einstein customer, it is important for you to know what data is being used in Sales Cloud, Service Cloud and Lightning Platform. This table lists the data that is used by each feature.

[Einstein and Data Usage in Commerce Cloud](#)

As an Einstein customer, it is important for you to know what data is being used in B2C Commerce, B2B Commerce, and D2C Commerce products. This table lists the data that is used by each feature.

Einstein and Data Usage in Sales Cloud, Service Cloud, Marketing Cloud Account Engagement, Marketing Cloud Growth, and Lightning Platform

As an Einstein customer, it is important for you to know what data is being used in Sales Cloud, Service Cloud and Lightning Platform. This table lists the data that is used by each feature.

Cloud, Product, or Package	Feature	Customer Data and Salesforce Objects Used	Usage Data Used	Global Model Used
Einstein Conversation Insights	Einstein Conversation Insights	Account, Contact, Opportunity, OpportunityHistory, OpportunityStage, User, VoiceCall, VideoCall, VideoCallRecording, VoiceCallRecording, VideoCallParticipant, meeting data	NA	Yes
Einstein Features (free Einstein applications included in versions of Sales Cloud, Service Cloud, and Lightning Platform)	Einstein Activity Capture –Email Insights	User email (anonymized)	NA	Yes
	Einstein Activity Capture – Recommended Connections	User emails and meeting events (recipient and participant metadata only)	NA	No
	Einstein Activity Capture – Signature Parser	Open-source and synthetic data (no customer data)	NA	No
	Einstein Article Recommendations	Default model doesn't use customer data. If enabled, customer-specific model uses Case, Article (Knowledge__kav), and CaseArticle.	CandidateAnswer (stores all articles recommended), EinsteinAnswerFeedback (stores customer interaction with recommended articles such as clicks and hovers)	No
	Einstein Bots (if NLP is enabled)	Utterances selected by customer. Object used: MLIIntentUtterance	NA	No
	Einstein Case Classification	Case	NA	No
	Einstein Case Wrap Up	Case, LiveChatTranscript	NA	No
Einstein Conversation Mining	Case, LiveChatTranscript, ConvReasonReportDefinition, ConvReasonReportSegmentDef, ConversationReasonGroup, ConversationReason, ConversationReasonExcerpt	ConversationReasonExcerpt (stores ID's and indexes from LiveChatTranscript or EmailMessage), engagement data based on usage (such as opens, clicks, exits) in the setup	No	

Cloud, Product, or Package	Feature	Customer Data and Salesforce Objects Used	Usage Data Used	Global Model Used
			flow and timestamps associated with them.	
	Einstein Deal Insights	Same as Einstein Opportunity Scoring	NA	No
	Einstein Opportunity Scoring	Account, Contact, CurrencyType, Event, EventRelation, Lead, Opportunity, OpportunityContactRole, OpportunityFieldHistory, OpportunityHistory, OpportunityLineItem, OpportunityScore, OpportunityScoringAIApplicationConfig, OpportunityStage, OpportunityTeamMember, PIAIApplicationConfig, PricebookEntry, Quote, RecordType, SalesAIScoreCycle, SalesAIScoreModelFactor, TaskOrganization, PermissionSet, PermissionSetAssignment, PermissionSetLicense, PermissionSetLicenseAssign, User, UserRole, Profile, OrgWideEmailAddress, MLModel, AIRecordInsight, AllInsightValue, AllInsightReason, SalesAIScoreCycle, SalesAIScoreAIFactor, AIApplication, MLPredictionDefinition, VoiceCall, VideoCall, VideoCallParticipant, OpportunitySplitType, OpportunitySplit objects, Product2, Product2History, Enterprise Territory Management objects, OpportunityLineItemSchedule, QuoteLineItem, Quote, Order, OrderItem, Contract, ContractLineItem, Invoice, InvoiceLine, Asset, AssetTag, Product2, ProductMedia. If Einstein Activity Capture is enabled: User emails, email insights, meeting data (events). If Einstein Conversation Insights is enabled: Insights.	Opportunity score user interaction feedback such as opportunity score rendered, hover on list view, and record home page	Yes
	Einstein Prediction Builder	Data selected by customer	NA	No
	Einstein Recommendation Builder	Data selected by customer	NA	No
Einstein Generative AI for Sales	Sales Emails	Account, Contact, Lead, Product, and User	Email, Engagement data based on send clicks	No

Cloud, Product, or Package	Feature	Customer Data and Salesforce Objects Used	Usage Data Used	Global Model Used
	Call Summaries	Video Call, Voice Call	Engagement data based on summaries processed	No
	Call Explorer	Video Call, Voice Call	Engagement data based on questions asked	No
	Sales Summaries	Account, AccountContactRelation, Case, Contact, Event, Lead, Opportunity, OpportunityCompetitor, OpportunityContactRole, OpportunityTeamMember, ScoreIntelligence, Task If Einstein Activity Capture is enabled: ActivityMetric, UnifiedActivity, UnifiedActivityRelation, and UnifiedEmail.	NA	No
Einstein Generative AI for Service	Einstein Work Summaries	LiveChatTranscript, VoiceCall, Case, Knowledge, Email, MessagingSession, ConversationEntry	NA	No
	Einstein Service Replies	LiveChatTranscript, VoiceCall, Case, Knowledge, Email, MessagingSession, ConversationEntry	NA	No
	Einstein AI-Generated Search Answers	Knowledge	Knowledge search terms, No knowledge search results (record IDs, query and document matching metadata), and knowledge article metadata.	No
Einstein Search	Einstein Search	NA	Search terms, search results (record IDs, query and document matching metadata, and user-MRU and document matching metadata), and org metadata. See How Does Einstein Search Use My Data .	Yes
Einstein Search for Knowledge	Einstein Search for Knowledge	NA	Knowledge search terms, No knowledge search results (record IDs, query and document matching metadata, and user-MRU and document matching metadata), and knowledge article metadata. See	Yes

Cloud, Product, or Package	Feature	Customer Data and Salesforce Objects Used	Usage Data Used	Global Model Used
			Enable Einstein Search for Knowledge.	
Einstein Vision and Language	Einstein Image Classification	Data selected by customer	NA	No
	Einstein Object Detection	Data selected by customer	NA	No
	Einstein OCR	Model is pretrained. Customer data isn't used.	NA	No
	Einstein Intent	Data selected by customer	NA	No
	Einstein Sentiment	Model is pretrained. Customer data isn't used.	NA	No
Account Engagement (Pardot) Einstein	Einstein Attribution	Account, Campaign, CampaignMember, CampaignMemberStatus, CampaignInfluence, CampaignInfluenceModel, Contact, Event, EventRelation, Lead, Opportunity, OpportunityHistory, OpportunityFieldHistory, OpportunityContactRole, OpportunityStage, PardotTenant, Profile, Task, AttributionTimeFrameConfig, AttrConversionPointConfig, OpportunityLineItem, PricebookEntry, CurrencyType, Organization, PermissionSet, PermissionSetAssignment, PermissionSetLicense, PermissionSetLicenseAssign, User, UserRole, Profile, MLModel, MLModelMetric, AIRecordInsight, AllInsightValue, AllInsightReason, AIApplication, MLPredictionDefinition. From Account Engagement: visitor, visitorActivity, lifecycleStage, lifecycleHistory, campaign, form, prospect.	NA	No
	Einstein Behavior Scoring	Account Engagement	NA	No
	Einstein Campaign Insights	Account, Campaign, CampaignInsight, CampaignInsightRationale, Contact, LandingPage, Lead, ListEmail, MarketingForm, PardotTenant, PredictionDefinition, RecordRecommendation, Organization, PermissionSet, PermissionSetAssignment, PermissionSetLicense, PermissionSetLicenseAssign, User, UserRole, Profile. From Account Engagement: visitor,	NA	No

Cloud, Product, or Package	Feature	Customer Data and Salesforce Objects Used	Usage Data Used	Global Model Used
		visitorActivity, lifecycleStage, lifecycleHistory, campaign, form, prospect.		
	Einstein Engagement Frequency	Analyzes the past 90 days' email engagement history for all business unit level subscribers over different frequencies. The engagement history that Einstein Engagement Frequency analyzes includes these factors: Engagement behavior such as sends, clicks, opens, unsubscribes, spam complaints, and associated timestamps. Data and metadata about customer sending patterns, including how campaigns are executed.	Engagement data based on usage (such as opens, clicks, unsubscribes) and timestamps associated with them	No
	Einstein Key Accounts Identification	Account, Campaign, CampaignMember, Contact, Event, EventRelation, Lead, Opportunity, OpportunityStage, OpportunityHistory, OpportunityContactRole, PardotTenant, Profile, Task, OpportunityLineItem, PricebookEntry, CurrencyType, ABEIAApplicationConfig, Organization, PermissionSet, PermissionSetAssignment, PermissionSetLicense, PermissionSetLicenseAssign, User, UserRole, Profile MLModel, MLModelMetric, AIRecordInsight, AllInsightValue, AllInsightReason, AIApplication, MLPredictionDefinition. From Account Engagement: visitor, visitorActivity, lifecycleStage, lifecycleHistory, campaign, form, prospect.	NA	No
	Einstein Lead Scoring for Account Engagement	Lead, LeadHistory, Task, Event, Account, Contact, RecordType, Organization, LeadIQConfiguration, AIApplication, AIModelDefinition, MLPredictionDefinition, MLDataDefinition	NA	Yes
	Einstein Send Time Optimization	Engagement behavior (sends, clicks, opens, unsubscribes, spam complaints) and associated timestamps. Data and metadata about customer sending patterns and how campaigns are executed.	Engagement data based on usage (such as opens, clicks, unsubscribes) and timestamps associated with them	No
	Einstein Assistant	Forms, landing pages, email subject lines, and body copy	Yes	No
Sales Cloud Einstein	Einstein Account Insights	External News, RecordRecommendation, AccountInsightNewsArticle, OpportunityInsight, AccountInsight, PredictionDefinition, Task, EventRelation, Event, Contact, Lead,	Account insights user interaction feedback such as account insights rendered, dismiss, undo	No

Cloud, Product, or Package	Feature	Customer Data and Salesforce Objects Used	Usage Data Used	Global Model Used
		AccountTeamMember, EntitySubscription, Account, Opportunity, OpportunityHistory, OpportunityContactRole, OpportunityStage, OpportunityTeamMember Organization, PermissionSet, PermissionSetAssignment, PermissionSetLicense, PermissionSetLicenseAssign, User, UserRole, Profile, OrgWideEmailAddress, RecordType, CurrencyType	dismiss, email, expand, collapse, open dropdown menu on Lightning Platform and Record Home	
Einstein Automated Contacts		ContactSuggestionInsight, OpportunityContactRoleSuggestionInsight, RecordRecommendation, PredictionDefinition, Contact, Lead, AccountTeamMember, EntitySubscription, Event, EventRelation, Task, Account, Opportunity, OpportunityHistory, OpportunityContactRole, OpportunityTeamMember, Organization, PermissionSet, PermissionSetAssignment, PermissionSetLicense, PermissionSetLicenseAssign, User, UserRole, Profile, OrgWideEmailAddress, RecordType, CurrencyType. If Einstein Activity Capture is enabled: User email and meetings.	Contact suggestion insights, opportunity contact role suggestion insights user interaction feedback such as contact suggestion insights rendered, dismiss, undo dismiss, expand, collapse, open dropdown menu, review suggestion, reject suggestion on Lightning Platform and Record Home	No
Einstein Forecasting		Same as Einstein Opportunity Scoring with the following additional entities: Individual, Period, ForecastingPrediction, ForecastingPredictionElement, ForecastingPredictionReason, ForecastingPredictionTrend, ForecastingType, OpportunitySplit, OpportunitySplitType, FiscalYearSettings, ForecastingSegmentationConfig, ForecastingTunerConfig, PeriodType, ForecastingQuota, ForecastingSourceDefinition, ForecastingTypeSource, ForecastingFilter, ForecastingFilterCondition	Forecasting prediction user interaction feedback such as forecasting prediction rendered, hover, and click prediction cell.	No
Einstein Opportunity Insights		RecordRecommendation, AccountInsightNewsArticle, OpportunityInsight, AccountInsight, PredictionDefinition, Task, EventRelation, Event, Contact, Lead, AccountTeamMember, EntitySubscription, Account, Opportunity, OpportunityHistory, OpportunityContactRole, OpportunityStage,	Opportunity insights user interaction feedback such as opportunity insights rendered, dismiss, undo dismiss, edit opportunity, email, expand, collapse, open dropdown menu on	No

Cloud, Product, or Package	Feature	Customer Data and Salesforce Objects Used	Usage Data Used	Global Model Used
		OpportunityTeamMember, Organization, PermissionSet, PermissionSetAssignment, PermissionSetLicense, PermissionSetLicenseAssign, User, UserRole, Profile, OrgWideEmailAddress, RecordType, CurrencyType. If Einstein Activity Capture is enabled: User email and meetings.	Lightning Platform and Record Home	
	Lead Scoring	Lead, LeadHistory, Task, Event, Account, Contact, RecordType, Organization, LeadIQConfiguration, AIApplication, AIModelDefinition, MLPredictionDefinition, MLDataDefinition	Lead score user interaction feedback such as opportunity score rendered, hover on list view, and record home page.	Yes
	Einstein Activity Capture –Email Insights, Einstein Activity Capture –Recommended Connections, Einstein Activity Capture – Signature Parser, Einstein Opportunity Scoring	See Einstein Features	See Einstein Features	See Einstein Features
Service Cloud Einstein	Einstein Reply Recommendations	LiveChatTranscript, QuickText	MLRetrainingFeedback (stores recommendations displayed and customer interaction with recommended replies). For example, posted, edited, marked not helpful.	No
	Einstein Article Recommendations, Einstein Bots (if NLP is enabled), Einstein Case Classification, Einstein Case Wrap Up	See Einstein Features	See Einstein Features	See Einstein Features

Cloud, Product, or Package	Feature	Customer Data and Salesforce Objects Used	Usage Data Used	Global Model Used
Sales Engagement	Einstein Activity Capture – Email Insights, Einstein Activity Capture –Recommended Connections, Einstein Activity Capture – Signature Parser	See Einstein Features	See Einstein Features	See Einstein Features
	Einstein Conversation Insights	See Einstein Conversation Insights	See Einstein Conversation Insights	See Einstein Conversation Insights
	Lead Scoring	See Sales Cloud Einstein	See Sales Cloud Einstein	See Sales Cloud Einstein
Salesforce Inbox	Einstein Activity Capture –Email Insights, Einstein Activity Capture – Recommended Connections, Einstein Activity Capture – Signature Parser	See Einstein Features	See Einstein Features	See Einstein Features
Marketing Cloud Growth	Co Create with Einstein	Campaigns, segments in Data Cloud, smails in Email Builder	Yes	No
	Einstein Send Time Optimization	Engagement behavior (sends, clicks, opens, unsubscribes, spam complaints) and associated timestamps. Data and metadata about customer sending patterns and how campaigns are executed.	No	Yes
	Einstein Metrics Guard	Email engagement (email sends, opens, clicks, unsubscribes, bounces, spam complaints), customer sending pattern data and metadata	No	Yes

Einstein and Data Usage in Commerce Cloud

As an Einstein customer, it is important for you to know what data is being used in B2C Commerce, B2B Commerce, and D2C Commerce products. This table lists the data that is used by each feature.

Global model types for Commerce Cloud

- Catalog Global Model
 - Machine learning model that works across catalogs of different customers. It pools together catalogs to better classify products or attributes of the products. This model uses the fields in the product catalogs (including name, description, primary category, category list, price, and custom attributes) and assets that are linked to in the product catalog (e.g., images).
 - This model is trained across Commerce Cloud customers that have not opted out of global modeling of catalogs. The Catalog Global Model will be used for customers that have opted out, but their data will not be used to train the model.
- Shopper Global Model
 - Machine learning model that combines shopper activities across stores of different customers to learn how to better predict, e.g., future shopper behavior, for better targeting.
- Merchant Global Model
 - Machine learning model that shares merchant activity/settings between customers, e.g., search dictionaries – Einstein suggests synonyms for generic product names based on cross-Merchant search activity. So, for instance, when a user searches for "couch" they also see "sofa".

The Customer has control over whether their data contributes to global models. Contact our [Commerce Cloud Support](#) team to manage how your data is used.

 **Note:** * Not all recommendation strategies use the Catalog Global Model. This applies to the Einstein Product Recommendations feature for B2C Commerce, B2B Commerce, and D2C Commerce.

Cloud or Package	Feature	Customer Data and Salesforce Objects Used	Uses Catalog Global Model	Uses Shopper Global Model	Uses Merchant Global Model
B2C Commerce	Einstein Product Recommendations	Shopper activity tracking and catalog data	Yes*	No	No
	Complete the Set	Shopper activity tracking and catalog data	Yes	No	No
	Einstein Commerce Insights	Shopper activity tracking and catalog data	No	No	No
	Einstein Search Suggestions	Shopper activity tracking and catalog data	No	No	No
	Einstein Predictive Sort	Shopper activity tracking and catalog data	Yes	No	No
	Einstein Dictionary Management	Shopper activity tracking and synonym dictionaries	No	No	Yes
B2B Commerce	Einstein Product Recommendations	Shopper activity tracking and catalog data	Yes*	No	No
	Einstein Semantic Search	Shopper activity tracking and catalog data	Yes	No	No
	Catalog Recommendations	Catalog data	No	No	No

Cloud or Package	Feature	Customer Data and Salesforce Objects Used	Uses Catalog Global Model	Uses Shopper Global Model	Uses Merchant Global Model
D2C Commerce	Einstein Product Recommendations	Shopper activity tracking and catalog data	Yes*	No	No
	Einstein Semantic Search	Shopper activity tracking and catalog data	Yes	No	No
	Category Recommendations	Catalog data	No	No	No

Set Up Einstein Search

Find out which objects and fields are searchable. Customize search settings, search result filters, and lookup search. Learn how to improve the search experience for users.

See [Work Faster and Smarter with Einstein Search](#).

EDITIONS

Available in: Lightning Experience and the Salesforce Mobile app

Available in:
Essentials, Professional, Enterprise, Performance,
and **Unlimited** Editions

Provide Maps and Location Services

Maps and location services uses Google Maps to display maps on standard address fields, enables creation of Visualforce maps, and helps users enter new addresses with autocomplete.

To generate a map image, an address must include the street and city fields and either the state, postal code, or the country. If an address field is missing any of the required information, a map won't display on the detail page of a record.

The map image on the address is static, but clicking the map image opens Google Maps in a new browser tab on the desktop, and opens a map app on a mobile device.

If your organization has Salesforce offline access enabled, a map doesn't display when a user's device is offline.

1. From Setup, enter *Maps* in the *Quick Find* box, select **Maps and Location Settings**, then click **Edit**.
2. Check *Enable Maps and Location Services*.
3. Click **Save**.

[Autocomplete Addresses](#)

When you enable autocomplete addresses, users of Salesforce app, Experience Cloud Aura, and Experience Cloud Lightning Web Runtime (LWR) sites can enter text in address fields and see possible matching addresses in a picklist.

[Considerations for Autocompleting Addresses](#)

Get familiar with these considerations before you enable the autocomplete address fields feature.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Professional, Enterprise, Performance,**
and **Unlimited** editions.

USER PERMISSIONS

To modify maps and location settings:

- Customize Application

Let Users Select States, Countries, and Territories from Picklists

State and country/territory picklists let users select states, countries and territories from predefined, standardized lists, instead of entering state and country/territory data into text fields. State and country/territory picklists offer faster and easier data entry. They help to ensure cleaner data that can be harnessed for other uses—in reports and dashboards, for example. They protect data integrity by preventing typos, alternate spellings, and junk data—even in records updated through the API.

Autocomplete Addresses

When you enable autocomplete addresses, users of Salesforce app, Experience Cloud Aura, and Experience Cloud Lightning Web Runtime (LWR) sites can enter text in address fields and see possible matching addresses in a picklist.

 **Note:** When a user selects an address from an autocomplete picklist result, the address is stored in the language assigned to that user.

1. From Setup, in the Quick Find box, enter *Maps*, select **Maps and Location Settings**, and then click **Edit**.
2. Select **Enable Maps and Location Services (powered by Google)**, and then select **Autocomplete standard address fields**.
3. Save your changes.

SEE ALSO:

[Considerations for Autocompleting Addresses](#)

Considerations for Autocompleting Addresses

Get familiar with these considerations before you enable the autocomplete address fields feature.

- The autocomplete address fields feature is available for all versions of the Salesforce mobile app, Lightning Experience, Experience Cloud Aura, and Experience Cloud LWR sites.
- To populate address details, Maps and Location Services uses the [Google Maps Geocoding API](#). If the Geocoding API can't map or parse an address component, then Maps and Location Services can't autocomplete the address field.
- Autocomplete address picklist results are optimized for these countries:
 - Australia
 - Brazil
 - Canada
 - France
 - Germany
 - Japan
 - Netherlands
 - Russia
 - Spain
 - Sweden
 - United Kingdom

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance,** and **Unlimited** Editions

USER PERMISSIONS

To modify maps and location settings:

- Customize Application

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance,** and **Unlimited** Editions

USER PERMISSIONS

To modify maps and location settings:

- Customize Application

- USA

- The autocomplete address fields feature doesn't appear on Experience Cloud sites when viewing a site as a guest user.

Let Users Select States, Countries, and Territories from Picklists

State and country/territory picklists let users select states, countries and territories from predefined, standardized lists, instead of entering state and country/territory data into text fields. State and country/territory picklists offer faster and easier data entry. They help to ensure cleaner data that can be harnessed for other uses—in reports and dashboards, for example. They protect data integrity by preventing typos, alternate spellings, and junk data—even in records updated through the API.

The states, countries, and territories in the picklists are based on ISO-3166 standard values, making them compatible with other applications.

State and country/territory picklists are available in the shipping, billing, mailing, and “other” address fields in the account, campaign members, contact, contract, lead, order, person accounts, quotes, and service contracts standard objects. The picklists are also available for managing users and companies in Setup. To use the picklists, first choose the country or territory, and then choose from the options that automatically populate the state or province picklist.

You can use the state and country/territory picklists in most places that state and country/territory fields are available in Salesforce, including:

- Record edit and detail pages
- List views, reports, and dashboards
- Filters, functions, rules, and assignments

State and country/territory picklists can also be searched, and they're supported in Translation Workbench.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **All Editions** except Database.com

State and Country/Territory Picklist Limitations

State and country/territory picklists include 239 countries and territories by default. They also include the states and provinces of the United States, Canada, Australia, Brazil, China, India, Ireland, Italy, and Mexico. State and country/territory picklists that contain more than 1,000 states or countries/territories can cause degraded performance. State and country/territory picklists don't work with:

- Salesforce to Salesforce
- Connect Offline
- Change sets

If your org uses Data.com, the Data.com records can contain states, countries, and territories not included in the standard state and country/territory picklists. If your org uses these states and countries, add them to the picklist before Data.com users can add or clean these records:

- American Samoa (AS)
- Guam (GU)
- Hong Kong (HK)
- Marshall Islands (MH)
- Netherlands Antilles (AN)
- Northern Mariana Islands (MP)
- Serbia and Montenegro (CS)
- United States Minor Outlying Islands (UM)

Picklist labels, not code values, are displayed in reports on state and country/territory fields. To display code value abbreviations wherever your users see state, country, and territory names, manually change your State Name or Country/Territory Name labels to your code values. (For editing instructions, see [Configure State and Country/Territory Picklists](#) on page 314.) You can access your records' state and country/territory code values by using the `StateCode` and `CountryCode` fields in Translation Workbench or the Data Loader.

Implementing State and Country/Territory Picklists

Here's how to transition from text-based state and country/territory fields to state and country/territory picklists.

- [Configure the state and country/territory values you want to use in Salesforce.](#)

We recommend this step because it allows you to customize state, country, and territory values. It ensures that state and country/territory data continues to work with the third-party systems you have integrated with Salesforce.

- [Scan your Salesforce data and customizations.](#)

Convert data and update customizations, such as list views, reports, and workflow rules, so that they continue to work with the new field type.

- [Convert the identified data.](#)

The conversion process lets you map the various values in your org to standard picklist values. For example, map U.S., USA, and United States to US.

- [Turn on the picklists for your users.](#)

We recommend that you configure state and country/territory picklist values, scan for affected data, and convert the identified data before taking this step. If don't complete all the steps, users can use the picklists in new records. However, existing data that is incompatible with the new format can compromise data consistency and integrity across the two field formats.

- Optionally, rescan and fix customizations or records that have been created or edited since your first scan.

[Integration Values for State and Country/Territory Picklists](#)

An integration value is a customizable text value that is linked to a state or country/territory code. Integration values for standard states, countries, and territories default to the full ISO-standard state, country, and territory names. Integration values function similarly to the API names of custom fields and objects. Configuring integration values allows integrations that you set up before enabling state and country/territory picklists to continue to work.

[Configure State and Country/Territory Picklists](#)

Configuring state and country/territory picklists means choosing which states and countries you want to be available in your Salesforce org. It lets you make state and country/territory picklists available for purposes like importing data, working with external systems, and accessing picklist data from the Metadata API.

[Standard Countries and Territories for Address Picklists](#)

Salesforce provides 239 countries and territories as standard for country/territory address picklists.

[Edit State, Country, and Territory Details](#)

To customize the states, countries, and territories in your picklists, edit their details.

[State and Country/Territory Picklists and the Metadata API](#)

If you're editing many state and country/territory picklist integration values, using the Metadata API is more efficient than editing values in Setup.

[Prepare to Scan State, Country, and Territory Data and Customizations](#)

Before switching from text-based state and country/territory fields to standardized state and country/territory picklists, scan your org to see how the change affects it. This discovery process shows you where and how state, country, and territory data appears in your org. The process also shows where this data is used in customizations, such as list views and reports. After you've analyzed the scan results, you can plan to convert your data, update your customizations, and turn on state and country/territory picklists.

[Scan State and Country/Territory Data and Customizations](#)

Scanning an organization for text-based state and country values reveals where and how text-based state and country data appears in existing records.

[Prepare to Convert State, Country, and Territory Data](#)

If your Salesforce organization includes text-based state, country, and territory values, you can convert that data to standardized picklist values.

[Convert State and Country/Territory Data](#)

To convert text-based state and country/territory data to picklist-compatible values, select specific text values and choose the standard values you want to map them to. For example, you can select all occurrences of "USA" and change them to "United States."

[Enable and Disable State and Country/Territory Picklists](#)

When you enable state and country/territory picklists, the picklists are immediately available to users. However, it can take some time for Salesforce to populate the ISO code fields on existing records. If users try to edit the state or country/territory on a record before the code field is populated, they're prompted to select a code value.

[State, Country, and Territory Picklist Fields](#)

Understand the state, country, and territory picklist fields.

[State and Country/Territory Picklist Field-Syncing Logic](#)

When you save records with state and country/territory picklist values, Salesforce syncs the records' integration and code values for states and countries. You can't directly edit state or country/territory integration values on record detail pages. You can directly edit records' state or country/territory integration values only with workflows, Apex code, API integrations, and so on.

[State and Country/Territory Picklist Error Messages](#)

Understand the errors that can occur when you try to save records with mismatched code and text values for states, countries, or territories.

Integration Values for State and Country/Territory Picklists

An integration value is a customizable text value that is linked to a state or country/territory code. Integration values for standard states, countries, and territories default to the full ISO-standard state, country, and territory names. Integration values function similarly to the API names of custom fields and objects. Configuring integration values allows integrations that you set up before enabling state and country/territory picklists to continue to work.

When you enable state and country/territory picklists, your text-typed `State/Province` and `Country` fields are repurposed as `Integration Value` fields. In reports and list views, your `Integration Value` fields are called `State/Province (text only)` and `Country (text only)`. In addition, for each of your `State/Province (text only)` and `Country (text only)` fields, a picklist-typed `State Code` or `Country Code` field is created. The state and country/territory picklist values set up in your organization determine the available values on these code fields.

Among the fields on each state or country/territory picklist value are `Active`, `Visible`, `Name`, `Code`, and `Integration Value`. All your state and country/territory picklists—for `Billing Address`, `Shipping Address`, and so on—can access

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions** except Database.com

the state and country/territory picklist values you create. Storing a state or country/territory code allows your records to access other information about your states, countries, and territories.

By default, `Name` and `Integration Value` fields for your states and countries contain identical values. The value in the `Name` field displays to users who interact with your picklist. `Integration Value` is used by:

- Apex classes and triggers
- Visualforce pages
- SOQL queries
- API queries and integrations
- Rules for assignment, AutoResponse, validation, and escalation
- Workflow rules
- Email templates
- Custom buttons and links
- Field set customizations
- Reports and list views

When you update a code value on a record, that record's `State/Province (text only)` or `Country (text only)` column is populated with the corresponding integration value. Likewise, when you update a state, or country (`text only`) column with a valid integration value, we keep the corresponding state or country/territory code column in sync. You can change your organization's integration values after you enable state and country/territory picklists. However, when you update your picklists' state and country/territory integration values, the integration values on your records aren't updated. Name values aren't stored on records. Instead, they're retrieved from Salesforce based on a record's `State Code` or `Country Code` value. If the states, countries, or territories in your picklists have different field values for `Name` and `Integration Value`, make sure your report or list view filters use the correct values. Use names in `State` and `Country` filters, and use integration values in `State (text only)` and `Country (text only)` filters. Otherwise, your reports can fail to capture all relevant records.

Edit your integration values in Setup or using the Metadata API. States', countries', and territories' `Name` fields are editable only in Setup. In the Metadata API, `Name` and `Integration Value` fields are called `label` and `integrationValue`, respectively.

SEE ALSO:

[Let Users Select States, Countries, and Territories from Picklists](#)

[Edit State, Country, and Territory Details](#)

[State and Country/Territory Picklist Field-Syncing Logic](#)

[State and Country/Territory Picklist Error Messages](#)

Configure State and Country/Territory Picklists

Configuring state and country/territory picklists means choosing which states and countries you want to be available in your Salesforce org. It lets you make state and country/territory picklists available for purposes like importing data, working with external systems, and accessing picklist data from the Metadata API.

Configuring picklists isn't required for you to enable state and country/territory picklists for users, but it's highly recommended. Configuring picklists helps ensure continuity and data integrity with existing state, country, and territory data and customizations.

When configuring states, countries, and territories, you start with countries and territories, and then drill down to their states or provinces. State and country/territory picklists include 239 countries and territories by default. They also include the states and provinces of the United States, Canada, Australia, Brazil, China, India, Ireland, Italy, and Mexico. State and country/territory picklists that contain more than 1,000 states or countries/territories can cause degraded performance. For the complete list of default countries, see [Standard Countries and Territories for Address Picklists](#).

Note:

- Integration values for state and country/territory picklists can also be configured through the Metadata API. For more information, read about the AddressSettings component in the *Metadata API Developer Guide*.
- State and country/territory picklists aren't supported in Salesforce change sets or packages. However, you can move integration value changes for state and country/territory picklists between sandbox and production orgs by using the Metadata API. To edit the existing states and countries in a picklist, configure your state and country/territory picklists in your sandbox org. Then, use the Metadata API to retrieve the sandbox configurations, and deploy them to your production org. You can't deploy new ISO codes or update ISO code values using any API.

1. From Setup, enter *State and Country/Territory Picklists* in the Quick Find box, then select **State and Country/Territory Picklists**.
2. On the State and Country/Territory Picklists page, click **Configure States, Countries, and Territories**.
3. On the Configure States, Countries, and Territories page, select from the following options:
 - **Active:** Makes the country or territory available in the Metadata API so that records that contain the country or territory can be imported. However, unless you also set it as visible, the country or territory isn't available to users in Salesforce. Otherwise, users can still make updates to an invisible country or territory through the API.
 - **Visible:** Makes the country or territory available to users in Salesforce. A country or territory must be active before you can make it visible.
4. Click **Edit** to view and edit details for the country, including to configure its states or provinces.
5. (Optional) Under Picklist Settings, select a `Default Country/Territory`. The Default Country/Territory automatically populates country/territory picklists for new records in your org, but users can select a different country or territory. Default countries and territories must be both active and visible.
6. To save your configuration, click **Save**.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions** except Database.com

USER PERMISSIONS

To configure state and country/territory picklists:

- **Modify All Data**

 **Note:** Active states and countries not marked `visible` are still valid filter lookup values. You can use invisible states and countries when creating filters in reports, list views, workflows, and so on.

SEE ALSO:

[Edit State, Country, and Territory Details](#)

[Let Users Select States, Countries, and Territories from Picklists](#)

[Integration Values for State and Country/Territory Picklists](#)

Standard Countries and Territories for Address Picklists

Salesforce provides 239 countries and territories as standard for country/territory address picklists.

Standard Countries

An asterisk (*) indicates that states or provinces are available for that country.

ISO Code	Country
AD	Andorra
AE	United Arab Emirates
AF	Afghanistan
AG	Antigua and Barbuda
AI	Anguilla
AL	Albania
AM	Armenia
AO	Angola
AQ	Antarctica
AR	Argentina
AT	Austria
AU	Australia*
AW	Aruba
AX	Aland Islands
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BD	Bangladesh
BE	Belgium
BF	Burkina Faso

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All** Editions except Database.com

ISO Code	Country
BG	Bulgaria
BH	Bahrain
BI	Burundi
BJ	Benin
BL	Saint Barthélemy
BM	Bermuda
BN	Brunei Darussalam
BO	Bolivia, Plurinational State of
BQ	Bonaire, Sint Eustatius, and Saba
BR	Brazil*
BS	Bahamas
BT	Bhutan
BV	Bouvet Island
BW	Botswana
BY	Belarus
BZ	Belize
CA	Canada*
CC	Cocos (Keeling) Islands
CD	Congo, the Democratic Republic of the
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Cote d'Ivoire
CK	Cook Islands
CL	Chile
CM	Cameroon
CN	China*
CO	Colombia
CR	Costa Rica
CU	Cuba

ISO Code	Country
CV	Cape Verde
CW	Curaçao
CX	Christmas Island
CY	Cyprus
CZ	Czechia
DE	Germany
DJ	Djibouti
DK	Denmark
DM	Dominica
DO	Dominican Republic
DZ	Algeria
EC	Ecuador
EE	Estonia
EG	Egypt
EH	Western Sahara
ER	Eritrea
ES	Spain
ET	Ethiopia
FI	Finland
FJ	Fiji
FK	Falkland Islands (Malvinas)
FO	Faroe Islands
FR	France
GA	Gabon
GB	United Kingdom
GD	Grenada
GE	Georgia
GF	French Guiana
GG	Guernsey
GH	Ghana

ISO Code	Country
GI	Gibraltar
GL	Greenland
GM	Gambia
GN	Guinea
GP	Guadeloupe
GQ	Equatorial Guinea
GR	Greece
GS	South Georgia and the South Sandwich Islands
GT	Guatemala
GW	Guinea-Bissau
GY	Guyana
HM	Heard Island and McDonald Islands
HN	Honduras
HR	Croatia
HT	Haiti
HU	Hungary
ID	Indonesia
IE	Ireland*
IL	Israel
IM	Isle of Man
IN	India*
IO	British Indian Ocean Territory
IQ	Iraq
IR	Iran, Islamic Republic of
IS	Iceland
IT	Italy*
JE	Jersey
JM	Jamaica
JO	Jordan
JP	Japan

ISO Code	Country
KE	Kenya
KG	Kyrgyzstan
KH	Cambodia
KI	Kiribati
KM	Comoros
KN	Saint Kitts and Nevis
KP	Korea, Democratic People's Republic of
KR	Korea, Republic of
KW	Kuwait
KY	Cayman Islands
KZ	Kazakhstan
LA	Lao People's Democratic Republic
LB	Lebanon
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
LY	Libya
MA	Morocco
MC	Monaco
MD	Moldova, Republic of
ME	Montenegro
MF	Saint Martin (French part)
MG	Madagascar
MK	North Macedonia
ML	Mali

ISO Code	Country
MM	Myanmar
MN	Mongolia
MO	Macao
MQ	Martinique
MR	Mauritania
MS	Montserrat
MT	Malta
MU	Mauritius
MV	Maldives
MW	Malawi
MX	Mexico*
MY	Malaysia
MZ	Mozambique
NA	Namibia
NC	New Caledonia
NE	Niger
NF	Norfolk Island
NG	Nigeria
NI	Nicaragua
NL	Netherlands
NO	Norway
NP	Nepal
NR	Nauru
NU	Niue
NZ	New Zealand
OM	Oman
PA	Panama
PE	Peru
PF	French Polynesia
PG	Papua New Guinea

ISO Code	Country
PH	Philippines
PK	Pakistan
PL	Poland
PM	Saint Pierre and Miquelon
PN	Pitcairn
PS	Palestine
PT	Portugal
PY	Paraguay
QA	Qatar
RE	Reunion
RO	Romania
RS	Serbia
RU	Russian Federation
RW	Rwanda
SA	Saudi Arabia
SB	Solomon Islands
SC	Seychelles
SD	Sudan
SE	Sweden
SG	Singapore
SH	Saint Helena, Ascension and Tristan da Cunha
SI	Slovenia
SJ	Svalbard and Jan Mayen
SK	Slovakia
SL	Sierra Leone
SM	San Marino
SN	Senegal
SO	Somalia
SR	Suriname
SS	South Sudan

ISO Code	Country
ST	Sao Tome and Principe
SV	El Salvador
SX	Sint Maarten (Dutch part)
SY	Syrian Arab Republic
SZ	Eswatini
TC	Turks and Caicos Islands
TD	Chad
TF	French Southern Territories
TG	Togo
TH	Thailand
TJ	Tajikistan
TK	Tokelau
TL	Timor-Leste
TM	Turkmenistan
TN	Tunisia
TO	Tonga
TR	Türkiye
TT	Trinidad and Tobago
TV	Tuvalu
TW	Taiwan
TZ	Tanzania, United Republic of
UA	Ukraine
UG	Uganda
US	United States*
UY	Uruguay
UZ	Uzbekistan
VA	Holy See (Vatican City State)
VC	Saint Vincent and the Grenadines
VE	Venezuela, Bolivarian Republic of
VG	Virgin Islands, British

ISO Code	Country
VN	Vietnam
VU	Vanuatu
WF	Wallis and Futuna
WS	Samoa
XK	Kosovo
YE	Yemen
YT	Mayotte
ZA	South Africa
ZM	Zambia
ZW	Zimbabwe

Edit State, Country, and Territory Details

To customize the states, countries, and territories in your picklists, edit their details.

To add or edit a state or province, navigate to its detail page through the detail page of its associated country.

In the case that the name of a country changes, that change is only automatically applied to new organizations. If you have an existing organization, you must manually update the country name.

1. From Setup, in the Quick Find box, enter *state*, and then select **State and Country/Territory Picklists**.
2. Click **Configure States, Countries, and Territories** and choose your action.
 - To add a country, click **New Country/Territory**.
 - To edit a country, click **Edit** and select the country.
 - To add a state or province to a country, click **Edit**, select the country, and click **New State**.
 - To edit a state or province, click **Edit**, then select the country and state, and click **Edit**.
3. Configure the State, Country, and Territory picklist fields.
4. Specify whether the state, country, or territory is **Active** and available in the Metadata API and can be imported.
5. For an active state, country, or territory, specify whether it's also **Visible** and available to users.
6. Save your changes.

SEE ALSO:

- [Let Users Select States, Countries, and Territories from Picklists](#)
- [Configure State and Country/Territory Picklists](#)
- [Integration Values for State and Country/Territory Picklists](#)
- [State and Country/Territory Picklists and the Metadata API](#)
- [State, Country, and Territory Picklist Fields](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All** Editions except Database.com

USER PERMISSIONS

To add or edit state, country, or territory details:

- **Modify All Data**

State and Country/Territory Picklists and the Metadata API

If you're editing many state and country/territory picklist integration values, using the Metadata API is more efficient than editing values in Setup.

You can use the Metadata API to edit existing states, countries, and territories in state and country/territory picklists. You can't use the Metadata API to create or delete new states, countries, or territories.

To edit the existing states and countries in a picklist, configure your state and country/territory picklists in your sandbox org. Then, use the Metadata API to retrieve the sandbox configurations, and deploy them to your production org. You can't deploy new ISO codes or update ISO code values using any API.

Search for "AddressSettings" in the [Metadata API Developer Guide](#) for information about working with state and country/territory picklists in the Metadata API.

SEE ALSO:

- [Integration Values for State and Country/Territory Picklists](#)
- [Edit State, Country, and Territory Details](#)

Prepare to Scan State, Country, and Territory Data and Customizations

Before switching from text-based state and country/territory fields to standardized state and country/territory picklists, scan your org to see how the change affects it. This discovery process shows you where and how state, country, and territory data appears in your org. The process also shows where this data is used in customizations, such as list views and reports. After you've analyzed the scan results, you can plan to convert your data, update your customizations, and turn on state and country/territory picklists.

Every org's discovery process is unique. For some orgs, transitioning from state and country/territory text fields to standardized picklists is straightforward and manageable. However, if state and country/territory metadata is used extensively throughout an org, the transition can be a complicated and time-consuming process. Salesforce recommends that you scan your org early and often so that you can transition smoothly to the new lists. Keep these recommendations and considerations in mind.

- Scanning doesn't convert data or fix your customizations. Convert your data separately, and update your customizations individually.
- You can continue to work normally in your org during the scan.
- The scanning process identifies affected managed packages but doesn't provide a mechanism for addressing packaging issues.
- Scanning doesn't find formulas that include state and country/territory metadata.
- You can't use display values in validation rules or workflow rules that use comparison formula functions. If your validation or workflow rules on state or country/territory fields use `BEGINS`, `CONTAINS`, `ISCHANGED`, or `REGEX`, use `ISPICKVAL` with state and country/territory code values in your comparison functions.
- Scanning doesn't find personal list views and reports that use state and country/territory metadata. Individual users must update those customizations themselves.
- Converted leads aren't scanned. State, country, and territory values aren't updated on converted lead records when you enable state and country/territory picklists.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions** except Database.com

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions** except Database.com

- Scan your org multiple times. After you update a customization, rescan to make sure that your changes fixed the problem and didn't create new ones.

SEE ALSO:

- [Scan State and Country/Territory Data and Customizations](#)
- [Let Users Select States, Countries, and Territories from Picklists](#)

Scan State and Country/Territory Data and Customizations

Scanning an organization for text-based state and country values reveals where and how text-based state and country data appears in existing records.

For example, you can see all the ways United States is saved as a text value, such as U.S., US, America, Estados Unidos, and even misspelled entries like Untied States. In addition, scanning shows you where state and country data is used in customizations, including:

- List views
- Reports
- Validation rules
- Custom buttons and links
- Workflow rules
- Email templates
- Field sets
- Apex classes and triggers
- Visualforce pages

When the scan is complete, you receive 2 emails with links to detailed reports: one on address data and one on customizations. After analyzing the reports, begin the tasks of converting existing data to picklist values and updating customizations so that they work with the new picklist fields.

1. From Setup, enter *State and Country/Territory Picklists* in the Quick Find box, then select **State and Country/Territory Picklists**.
2. On the State and Country/Territory Picklists setup page, click **Scan for state and country/territory data**
3. On the Scan for Affected Data and Customizations page, click **Scan for State and Country/Territory Data**.
4. Wait for an email that contains the results.

Depending on the size and complexity of your organization, the results take anywhere between a few minutes and a few hours to generate.

 **Note:** The emails are sent from noreply@salesforce.com. They have the subject line, "Salesforce Address Data Scan" or "Salesforce Address Customization Scan." If you don't receive the emails, make sure that they weren't caught in a spam filter.

5. Click the link in each email to go to a document that contains the report of affected data or customizations.
6. On the Document detail page, click **View file**.

SEE ALSO:

- [Let Users Select States, Countries, and Territories from Picklists](#)

EDITIONS

Available in: both Salesforce Classic (**not available in all orgs**) and Lightning Experience

Available in: **All** Editions except Database.com

USER PERMISSIONS

To scan state and country data and customizations:

- Modify All Data
- AND
- Create Documents

Prepare to Convert State, Country, and Territory Data

If your Salesforce organization includes text-based state, country, and territory values, you can convert that data to standardized picklist values.

Converting existing data allows you to keep working with the data after you switch to picklists. For example, say you have a report that culls all your sales reps' leads in Washington state. The report is generated from state picklist value Washington. To ensure that records with text-based state values such as Wash., WA, and Washington are included in the report, convert text-based state data to standardized picklist values.

Converting existing state, country, and territory text data into standardized picklist values helps ensure data integrity after you enable picklists in your organization. Your users encounter validation errors when saving records that contain state, country, or territory values that aren't in your picklists.

Also, reports become unreliable when records created before you enable state and country/territory picklists contain different state, country, and territory values than records created using picklists.

When you convert data, Salesforce starts with countries and territories, then goes on to states. As you go through the conversion process, here are a few things to keep in mind:

- Save frequently. You can exit the conversion tool and return to it at any time.
- You can continue to work normally in your organization while converting data.
- You can't convert data while you're scanning for affected data and customizations, or while state or country/territory picklists are being deployed.
- Steps can be repeated and undone at any time until you enable the picklists for users. After the picklists are enabled, you can't undo the conversion.
- If you use Data.com Clean, we recommend that you suspend Clean jobs until the conversion is finished.

SEE ALSO:

[Convert State and Country/Territory Data](#)

[Let Users Select States, Countries, and Territories from Picklists](#)

Convert State and Country/Territory Data

To convert text-based state and country/territory data to picklist-compatible values, select specific text values and choose the standard values you want to map them to. For example, you can select all occurrences of "USA" and change them to "United States."

Before you convert state, country, and territory values in State and Country/Territory Picklists setup, [configure the picklists for your org](#). That way, the data in your org is consistent and accurate when you enable picklists, because all new and updated records use your specified integration value.

Convert countries first, and then states and provinces.

You can convert up to 2,000 country/territory values and up to 2,000 state values. However, state and country/territory picklists that contain more than 1,000 states or countries can degrade performance.

1. From Setup, enter *State and Country/Territory Picklists* in the Quick Find box, then select **State and Country/Territory Picklists**.
2. On the State and Country/Territory Picklists page, click **Convert identified data**.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions** except Database.com

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions** except Database.com

USER PERMISSIONS

To convert text-based state and country/territory data:

- Modify All Data

Salesforce opens the Convert States, Countries, and Territories page. This page displays all the country and territory text values that appear in your org and the number of times each value is used.

3. Select **Change** for one or more values you want to convert. For example, select **Change** for all the iterations of United States.
4. In the **Change To** area, choose the country or territory that you want to convert the text values to and click **Save to Changelist**.

 **Note:** If you map states or countries to `Unknown` value, users see states and countries in their records. However, your users encounter errors when they save records, unless they change each state, country, and territory to a valid value before saving.

5. Repeat Steps 3 and 4 for other country and territory values, such as for Canada. Salesforce tracks planned changes in the Changelist area.
6. When all the countries are mapped, click **Next** to convert state values. Use the Country of Origin column to identify the country or territory associated with that state or province.
7. To convert the values and turn on state and country/territory picklists in your org, click **Finish and Enable Picklists** on the Confirm Changes page. Or, to return to the State and Country/Territory Picklists page, click **Finish**.

A few words about undo:

- On the Convert Countries or Convert States page, click **Undo** at any time to revert values in the changelist.
- On the Convert States page, click **Previous** to return to the Convert States, Countries, and Territories page and change country and territory mappings.
- You can convert state, country, and territory values even after clicking **Finish**. After picklists are enabled, however, you can no longer edit your conversion mappings.

SEE ALSO:

[Let Users Select States, Countries, and Territories from Picklists](#)

Enable and Disable State and Country/Territory Picklists

When you enable state and country/territory picklists, the picklists are immediately available to users. However, it can take some time for Salesforce to populate the ISO code fields on existing records. If users try to edit the state or country/territory on a record before the code field is populated, they're prompted to select a code value.

1. From Setup, enter *State and Country/Territory Picklists* in the Quick Find box, then select **State and Country/Territory Picklists**.
2. On the State and Country/Territory Picklists setup page, click **Enable Picklists for Address Fields** to turn on the picklists.

 **Note:**

- You can also enable state and country/territory picklists when you finish converting existing, text-based data to picklist values. See [Convert State and Country/Territory Data](#).

3. To turn off state and country/territory picklists, click **Disable** on the State and Country/Territory Picklists setup page.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions** except Database.com

USER PERMISSIONS

To turn state and country/territory picklists on and off:

- **Modify All Data**

! **Important:** If you disable state and country/territory picklists:

- For records that you haven't saved since enabling picklists, state and country/territory values revert to their original text values.
- For records that you've saved since enabling picklists, state, country, and territory integration values replace original text values.
- References to state and country/territory picklists in customizations—such as workflow field updates, email templates, and Visualforce pages—become invalid.
- Columns and filters that refer to picklist fields in reports and list views disappear.
- You can't edit state and country/territory fields in reports.

SEE ALSO:

[Let Users Select States, Countries, and Territories from Picklists](#)

State, Country, and Territory Picklist Fields

Understand the state, country, and territory picklist fields.

Section Title

Field	Description
Country/Territory Name	The ISO-standard name that appears in the Salesforce user interface.
Country/Territory Code	The two-letter ISO-standard code. If you change an ISO code, the new value must be unique. Codes are case insensitive and must contain only ASCII characters and numbers. You can't edit the ISO codes of standard states or countries. You can edit the country or territory codes of custom states, countries, and territories only before you enable those states, countries, and territories for your users.
Country/Territory Phone Code	The one- to three-digit international phone number format for this country or territory without the plus sign or other prefix.
Integration Value	<p>A customizable text value that is linked to a state, country, or territory code. Integration values for standard states, countries, and territories default to the full ISO-standard names. Integration values function like the API names of custom fields and objects and enable existing integrations to continue to work even after you set up the picklist.</p> <p>You can edit integration values to match values that you use elsewhere in your organization. For example, a workflow rule uses <code>USA</code> instead of the default <code>United States</code> as the country name. If you manually set the integration value for country/territory code <code>US</code> to <code>USA</code>, the workflow rule doesn't break when you enable state and country/territory picklists.</p> <p>When you update a code value on a record, that record's <code>State/Province (text only)</code> or <code>Country (text only)</code> column is populated with the corresponding integration value. And, when you update a state, or country (<code>text only</code>) column with a valid integration value, the corresponding state, or country/territory code column stays in sync. You can change your organization's integration values after you enable state and country/territory picklists. But when you update your picklists' state and country/territory integration values, the integration values on your records aren't</p>

	updated. Name values aren't stored on records. Instead, they're retrieved based on a record's <code>State Code</code> or <code>Country Code</code> value. If the states, countries, or territories in your picklists have different field values for <code>Name</code> and <code>Integration Value</code> , make sure your report or list view filters use the correct values. Use names in <code>State</code> and <code>Country</code> filters, and use integration values in <code>State (text only)</code> and <code>Country (text only)</code> filters. Otherwise, your reports can fail to capture all relevant records.
<code>Active</code>	Makes the state, country, or territory available in the Metadata API so that records can be imported that contain the country. But records aren't available to users in Salesforce unless set to visible.
<code>Visible</code>	Makes the state, country, or territory record available to users in Salesforce. To make a record visible, first make it active.

State and Country/Territory Picklist Field-Syncing Logic

When you save records with state and country/territory picklist values, Salesforce syncs the records' integration and code values for states and countries. You can't directly edit state or country/territory integration values on record detail pages. You can directly edit records' state or country/territory integration values only with workflows, Apex code, API integrations, and so on.

Your Change	Result
You update a record's state or country/territory code to a valid value.	Salesforce updates the record's state or country/territory integration value to match the code.
You update a record's state or country/territory integration value to a valid value.	Salesforce updates the record's state or country/territory code to match the integration value.
You remove a record's country/territory code, but don't remove the corresponding state code.	Salesforce removes the record's state code and the state and country/territory integration values.
You create or update a record with state and country/territory values. The new state isn't in the new country.	No changes are saved. You get an error message.
You update the state or country/territory integration and code values on an existing record. The new integration and code values don't match.	No changes are saved. You get an error message.
You create a record with mismatched state or country/territory integration and code values.	Salesforce updates your new record's integration value to match the code value.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions** except Database.com

SEE ALSO:

- [Let Users Select States, Countries, and Territories from Picklists](#)
- [Integration Values for State and Country/Territory Picklists](#)
- [State and Country/Territory Picklist Error Messages](#)

State and Country/Territory Picklist Error Messages

Understand the errors that can occur when you try to save records with mismatched code and text values for states, countries, or territories.

Error	Cause
Invalid country specified for field	Your country/territory code doesn't match an existing country or territory.
There's a problem with this country, even though it may appear correct. Please select a country from the list of valid countries.	Your country/territory integration value doesn't match an existing country. Or, the country/territory value was mapped to <code>Unknown</code> value during data conversion.
Mismatched integration value and ISO code for field	Your code and integration values match different states or countries.
A country must be specified before specifying a state value for field	Your record has a state code or integration value but no country/territory code. You can't save a state without a corresponding country.
The existing country doesn't recognize the state value for field	Your state code and integration values belong to a state in a different country.
Invalid state specified for field	Your state code doesn't match an existing state.

SEE ALSO:

- [Let Users Select States, Countries, and Territories from Picklists](#)
- [Integration Values for State and Country/Territory Picklists](#)
- [State and Country/Territory Picklist Field-Syncing Logic](#)

Customize Reports and Dashboards

Set up reports and dashboards to deliver information to your users in the ways that work best for them.

To get to this page, from Setup, enter *Reports* in the **Quick Find** box, then select **Reports and Dashboards Settings**.

[Provide Convenience Features for Your Report and Dashboard Users](#)

You can enable or disable several user interface features that may help your users get more out of reports and dashboards. These settings are for convenience and ease of use; they don't affect the data returned in your reports and dashboards.

[Let Users Attach Files to Report Subscriptions](#)

Let users who subscribe to reports choose to receive report results as a formatted spreadsheet (.XLSX) or a comma-separated (.CSV) file attached to the subscription email. The email itself includes the report name in the subject line, but there is no email body. Row-level record details are included in the attached file instead.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions** except Database.com

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: all editions except **Database.com**

USER PERMISSIONS

To modify report and dashboard settings:

- [Customize Application](#)

[Hide the Embedded Salesforce Classic Report Builder in Lightning Experience](#)

Give your users the complete Lightning experience by hiding the embedded Salesforce Classic report builder.

[Let Users Subscribe to Report Notifications](#)

Allow users to subscribe to reports to be notified whenever certain metrics meet conditions they specify.

[Customize Report and Dashboard Email Notifications](#)

Enable report and dashboard email notifications to allow all internal and community (portal) users specified as recipients to receive report and dashboard notifications. If this option isn't enabled, only internal Salesforce users can receive the notifications. This option is available to Enterprise, Unlimited, and Performance Edition organizations that have a Customer Portal or partner portal set up as part of Experience Cloud.

[Set Up a Custom Report Type](#)

A *report type* defines the set of records and fields available to a report based on the relationships between a primary object and its related objects. Reports display only records that meet the criteria defined in the report type.

[Bulk Move Reports or Dashboards with Metadata API](#)

You can move reports or dashboards between folders and subfolders in Lightning Experience. If you want to move reports or dashboards in bulk, use Metadata API.

[Set Up Historical Trend Reporting](#)

Historical trend reporting allows you to track how field values have changed over time.

[Upgrade the Report Wizard](#)

Report builder, a powerful drag-and-drop editor, is the standard tool for creating and editing reports. If your organization is still using the old report wizard, you should upgrade to report builder.

SEE ALSO:

[Upgrade the Report Wizard](#)

Provide Convenience Features for Your Report and Dashboard Users

You can enable or disable several user interface features that may help your users get more out of reports and dashboards. These settings are for convenience and ease of use; they don't affect the data returned in your reports and dashboards.

[Let Users See Report Headers While Scrolling](#)

Floating report headers keep column and row headings in sight no matter how far users scroll in report results.

[Help Users Find Dashboards Quickly](#)

Dashboard finder uses auto-complete to help users quickly find dashboards in the Dashboards tab, just by entering the first few letters of its name in the search filter.

[Let Users Post Dashboard Widgets in Chatter](#)

Dashboard widget snapshots let users post static images of dashboard widgets to Chatter feeds, making the snapshot visible to all users.

[Exclude the Confidential Information Disclaimer from Reports](#)

By default, report footers include a disclaimer that reads "Confidential Information - Do Not Distribute". The disclaimer reminds users to be mindful of who they share reports with, helping to ensure that third parties don't view your reports. At your discretion, exclude the disclaimer from formatted report exports in Lightning Experience and from run pages and printable views in Salesforce Classic.

USER PERMISSIONS

To modify report and dashboard settings:

- [Customize Application](#)

Let Users See Report Headers While Scrolling

Floating report headers keep column and row headings in sight no matter how far users scroll in report results.

With floating report headers, users can scroll to the bottom of lengthy reports without having to scroll back to the top to view the names of the column headings.

Users can also click floating report headers to sort data in a specific column. When users sort data by clicking a floating report heading, the report refreshes and redirects users to the beginning of report results.

Floating headers are available for tabular, summary, and matrix reports.

1. From Setup, enter *Reports* in the **Quick Find** box, then select **Reports and Dashboards Settings**.
2. Select or deselect **Enable Floating Report Headers**.
3. Click **Save**.

Help Users Find Dashboards Quickly

Dashboard finder uses auto-complete to help users quickly find dashboards in the Dashboards tab, just by entering the first few letters of its name in the search filter.

All dashboards matching that text are dynamically displayed in the drop-down list. The list first shows dashboards the user viewed recently, and then other dashboards appear in alphabetical order by folder. The first 1000 results are shown in a single list; above 1000, results are shown 500 per page. Users only see dashboards in folders they can access. Disable this option to use the static drop-down list instead.

This option is enabled by default.

1. From Setup, enter *Reports* in the **Quick Find** box, then select **Reports and Dashboards Settings**.
2. Select or deselect **Enable Dashboard Finder**.
3. Click **Save**.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Essentials, Group** (View Only), **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Group** (View only), **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

Let Users Post Dashboard Widgets in Chatter

Dashboard widget snapshots let users post static images of dashboard widgets to Chatter feeds, making the snapshot visible to all users.

Important: This option lets users override dashboard visibility settings, making snapshots visible to all Chatter users. Though this makes it easy to share time-specific data without having to add people to dashboard folders, be aware that users can inadvertently post sensitive or confidential information.

1. Make sure that Chatter feed tracking for dashboards is enabled.
2. From Setup, enter *Reports* in the Quick Find box, and select **Reports and Dashboards Settings**.
3. Select or deselect **Enable Dashboard Component Snapshots**.

Exclude the Confidential Information Disclaimer from Reports

By default, report footers include a disclaimer that reads “Confidential Information - Do Not Distribute”. The disclaimer reminds users to be mindful of who they share reports with, helping to ensure that third parties don’t view your reports. At your discretion, exclude the disclaimer from formatted report exports in Lightning Experience and from run pages and printable views in Salesforce Classic.

1. From Setup, enter *Reports and Dashboards Settings* in the Quick Find box, then select **Reports and Dashboards Settings**.
2. Select **Exclude Disclaimer from Formatted Report Exports in Lightning Experience** and **Exclude Disclaimer from Report Run Pages and from Printable View Pages (Salesforce Classic Only)**.
3. Click **Save**.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Group** (View Only), **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Group** (View Only), **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

Let Users Attach Files to Report Subscriptions

Let users who subscribe to reports choose to receive report results as a formatted spreadsheet (.XLSX) or a comma-separated (.CSV) file attached to the subscription email. The email itself includes the report name in the subject line, but there is no email body. Row-level record details are included in the attached file instead.

 **Note:** As a beta feature, Report Subscription Attachments is a preview and isn't part of the "Services" under your Main Services Agreement with Salesforce. Use this feature at your sole discretion, and make your purchase decisions only on the basis of generally available products and features. Salesforce doesn't guarantee general availability of this feature within any particular time frame or at all, and we can discontinue it at any time. This feature is for evaluation purposes only, not for production use. It's offered as is and isn't supported, and Salesforce has no liability for any harm or damage arising out of or in connection with it. All restrictions, Salesforce reservation of rights, obligations concerning the Services, and terms for related Non-Salesforce Applications and Content apply equally to your use of this feature. You can provide feedback and suggestions for Report Subscription Attachments in the [IdeaExchange](#) or in the [Trailblazer Community](#). For information on enabling this feature in your org, contact Salesforce.

1. From Setup, enter *Reports* in the Quick Find box, then select **Reports and Dashboards Settings**.
2. Select *Let users attach reports as files to report subscription emails in Lightning Experience*.
3. Click **Save**.

While subscribing to a report, users with the requisite user permissions can now choose to attach a file containing report results to subscription emails.

 **Note:** Even if your org participated in the Spring '20 closed beta, to attach files to report subscription emails, an admin must enable this feature from setup.

Hide the Embedded Salesforce Classic Report Builder in Lightning Experience

Give your users the complete Lightning experience by hiding the embedded Salesforce Classic report builder.

Available in: Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Available in: Enhanced Folder Sharing

The Lightning report builder is a powerful, intuitive tool for analyzing Salesforce data. Users can group, filter, and summarize records to answer business questions like "Which lead source generates the most closed opportunities?"

1. From Setup, enter *Reports* in the Quick Find box, then select **Reports and Dashboards Settings**.
2. Select **Hide the embedded Salesforce Classic report builder in Lightning Experience**.
3. Click **Save**.

EDITIONS

Available in: Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

The Salesforce Classic report builder is hidden in Lightning Experience. Users no longer see the **New Report (Salesforce Classic)** and **Edit (Salesforce Classic)** buttons on the Reports tab in Lightning Experience.

Let Users Subscribe to Report Notifications

Allow users to subscribe to reports to be notified whenever certain metrics meet conditions they specify.

1. From Setup, enter *Report Notifications* in the Quick Find box, then select **Report Notifications**.
2. Select the option to enable report notifications.
3. Click **Save**.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **All** editions except **Database.com**

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

Customize Report and Dashboard Email Notifications

Enable report and dashboard email notifications to allow all internal and community (portal) users specified as recipients to receive report and dashboard notifications. If this option isn't enabled, only internal Salesforce users can receive the notifications. This option is available to Enterprise, Unlimited, and Performance Edition organizations that have a Customer Portal or partner portal set up as part of Experience Cloud.

1. From Setup, enter *Email Notifications* in the Quick Find box, then select **Email Notifications**.
2. To enable email notifications for your organization clear, select **Allow Community Users to Receive Reports and Dashboards by Email**.
3. Click **Save**.

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

Set Up a Custom Report Type

A *report type* defines the set of records and fields available to a report based on the relationships between a primary object and its related objects. Reports display only records that meet the criteria defined in the report type.

When an administrator creates a custom report type, the type becomes available to other users when creating a report. For example, if an administrator creates a report type that shows only job applications that have an associated resume, applications without resumes are omitted from reports based on that type. An administrator can also show records with or without related records—for example, applications with or without resumes. In this case, all applications, with or without resumes, are available to reports using that type.

When you're done creating your report type, consider ways you can do more with it:

- Add the custom report type to apps you upload to AppExchange.
- Users designated as a translator with the View Setup and Configuration permission can translate custom report types using the Translation Workbench.

1. [Create a Custom Report Type](#)

Choose the primary object you'd like your new report type to support, then give it a name and a useful description. Mark it as "in development" until you're ready to make it available for users to create reports.

2. [Add Child Objects to Your Custom Report Type](#)

To enable reports to pull data from more than just the primary object, consider adding one or more related objects to your report type.

3. [Design the Field Layout for Reports Created from Your Custom Report Type](#)

After you define a custom report type and choose its object relationships, specify the standard and custom fields available on reports for the custom report type.

4. [Manage Custom Report Types](#)

After you create a custom report type, you can customize, edit, and delete it.

5. [Limits on Report Types](#)

Custom report types are subject to some limits for high performance and usability.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

Available in: Enhanced Folder Sharing and Legacy Folder Sharing

USER PERMISSIONS

To create, update, and delete custom report types:

- [Manage Custom Report Types](#)

Create a Custom Report Type

Choose the primary object you'd like your new report type to support, then give it a name and a useful description. Mark it as "in development" until you're ready to make it available for users to create reports.

1. From Setup, enter *Report Types* in the *Quick Find* box, then select **Report Types**.
2. If the Custom Report Type welcome page opens, click **Continue**.
3. Click **New Custom Report Type**.
4. Select the *Primary Object* for your custom report type.



Tip:

- You can choose from all objects—even the objects that you don't have permission to view. This flexibility lets you build report types for a variety of users.
- After you save a report type, you can't change the primary object.
- If the primary object on a report type is a custom or external object, and that object is deleted, the report type and reports created from it are deleted.
- If you remove an object from a report type, all references to that object and its associated objects are removed from the reports and dashboards based on that type.
- The name of the primary object is derived from the plural label field. The names of any related objects are derived from either the related list label field or the custom field that defines its relationship to the primary object.
- In Essentials edition, when adding a child object, you can't change the relationship with the primary object.
- To create custom report types from which users can report on your organization's reports and dashboards, select *Reports or Dashboards* from the *Primary Object* dropdown list.

5. Enter the *Report Type Label* and the *Report Type Name*.

The label can be up to 50 characters long. If you enter a name that is longer than 50 characters, the name gets truncated. The name is used by SOAP API.

6. Enter a description for your custom report type, up to 255 characters long. If you enter a name that is longer than 255 characters, the name gets truncated.

Provide a meaningful description so users have a good idea of which data is available for reports. For example: *Accounts with Contacts. Report on accounts and their contacts. Accounts without contacts are not shown..*

7. Select the category in which you want to store the custom report type.

8. Select a *Deployment Status*:

- Choose *In Development* during design and testing as well as editing. The report type and its reports are hidden from all users except user with the "Manage Custom Report Types" permission. Only users with that permission can create and run reports using report types in development.
- Choose *Deployed* when you're ready to let all users access the report type.



Note: A custom report type's *Deployment Status* changes from *Deployed* to *In Development* if its primary object is a custom or external object whose *Deployment Status* similarly changes.

EDITIONS

Available in: Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

Available in: Enhanced Folder Sharing and Legacy Folder Sharing

USER PERMISSIONS

To create and update custom report types:

- **Manage Custom Report Types**

9. Click **Next**.

- A developer can edit a custom report type in a managed package after it's released, and can add new fields. Subscribers automatically receive these changes when they install a new version of the managed package. However, developers can't remove objects from the report type after the package is released. If you delete a field in a custom report type that's part of a managed package and the deleted field is part of bucketing or used in grouping, you receive an error message.
- Custom fields that you add to a Salesforce object in Setup are added automatically to all of the custom report types that based on that object. New fields that are deployed as part of a package aren't added to custom report types.

Add Child Objects to Your Custom Report Type

To enable reports to pull data from more than just the primary object, consider adding one or more related objects to your report type.

1. Click the box under the primary object.

2. Select a child object.

Only related objects are shown.



Note: The name of the primary object is derived from the plural label field. The names of any related objects are derived from either the related list label field or the custom field that defines its relationship to the primary object.

3. For each child object, select one of the following criteria:

- Each "A" record must have at least one related "B" record. Only parent records with child records are shown in the report.
- "A" records may or may not have related "B" records. Parent records are shown, whether they have child records or not.

When Users are the primary object, select child objects by field—for example, Accounts (Account Owner) or Accounts (Created By).



Note: In Essentials edition, you can't change the type of relationship for a custom report type. Each "A" record must have a related "B" record.

4. Add up to three child objects.

The number of children depends on the objects you choose.

5. Click **Save**.



Example:

- If you select **A may or may not have object B records**, then all subsequent objects automatically include the "may-or-may-not" association on the custom report type. For example, assume that Accounts is the primary object and Contacts is the secondary object. If you select that Accounts may or may not have Contacts, then any tertiary and quaternary objects included on the custom report type default to "may-or-may-not" associations.
- When object A doesn't have object B, blank fields appear on report results for object B. For example, if a user runs a report on Accounts with or without Contacts, Contact fields appear as blank for the accounts that don't have contacts.
- On reports where object A may or may not have object B, you can't use the OR condition to filter across multiple objects. For example, if you select *Account Name starts with M OR Contact First Name starts with M*, an error message informs you that your filter criteria are incorrect.
- (Salesforce Classic only) For custom report types where object A may or may not have object B, the Row Limit option on tabular reports shows only the fields for the primary object.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Available in: Enhanced Folder Sharing and Legacy Folder Sharing

USER PERMISSIONS

To create and update custom report types:

- Manage Custom Report Types

Examples:

- In an Accounts with or without Contacts report, the Row Limit option shows only fields from Accounts.
- In an Accounts with Contacts with or without Cases report, the Row Limit option shows only fields from Accounts and Contacts.

Design the Field Layout for Reports Created from Your Custom Report Type

After you define a custom report type and choose its object relationships, specify the standard and custom fields available on reports for the custom report type.

 **Note:** Custom fields appear in custom report types only if they've been added to that report type's page layout.

1. From Setup, enter *Report Types* in the Quick Find box, then select **Report Types**.
2. If the Custom Report Type welcome page opens, click **Continue**.
3. Select the custom report type that you want to edit and click **Edit Layout** on the Fields Available for Reports section. To preview which fields display on the Select Columns page, click **Preview Layout**

When previewing the layout, all fields and objects are displayed, including fields and objects that you don't have permission to access. However, you can access only the data that is stored in the fields or objects that you have permission to access.

4. Select fields from the right box and drag them to a section on the left. You can view an object's fields by selecting it from the View dropdown list.

 **Warning:** If you add custom fields with the same API name from different objects, only one of the fields displays in the reports. For example, adding both `Account.Custom_Field__c` and `Opportunity.Custom_Field__c` results in one `Custom_Field__c` visible on reports.

5. Optionally, click **Add fields related via lookup** to display the Add Fields Via Lookup overlay and add fields via the lookup relationship the object selected in the `View` dropdown list.
6. Remove a field by dragging it from the layout to the right box. When you remove a field, it's removed from all reports based on the report type. A report in which the removed field was used in filter logic displays an error message when viewed.
7. Arrange fields in sections as you want them to appear to users. Fields not added to a section are unavailable to users when they generate reports from this report type.
8. Click **Preview Layout** and use the legend to determine which fields are included on the layout, added to the report by default, and added to the layout via a lookup relationship.

Users can view roll-up summary fields on reports that include data from fields they don't have access to view. For example, a user that doesn't have access to view the `Price` field on an opportunity product can view the `Total Price` field on opportunity reports if he or she has access to the `Total Price` field.

9. To rename or set which fields are selected by default for users, select one or more fields and click **Edit Properties**.
10. To rename the sections, click **Edit** next to an existing section, or create a section by clicking **Create New Section**.
11. Click **Save**.

When you're working with lookup fields, consider these tips:

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

Available in: Enhanced Folder Sharing and Legacy Folder Sharing

USER PERMISSIONS

To create and update custom report types:

- **Manage Custom Report Types**

- A lookup field is a field on an object that displays information from another object. For example, the `Contact Name` field on an account.
 - A custom report type can contain fields available via lookup through four levels of lookup relationships. For example, for an account, you can get the account owner, the account owner's manager, the manager's role, and that role's parent role.
 - You can add fields via lookup that are associated with objects included in the custom report type. For example, if you add the accounts object to the custom report type, then you can add fields from objects to which accounts have a lookup relationship.
 - Selecting a lookup field on the Add Fields Via Lookup overlay lets you access additional lookup fields from other objects to which there's a lookup relationship. For example, if you select the `Contact Name` field from cases, you can then select the `Account` field. You can do so because accounts have a lookup relationship to contacts that have a lookup relationship to cases.
 - The fields displayed in the Add Fields Via Lookup overlay don't include lookup fields to objects in the report type. For example, if accounts are the primary object on your custom report type and contacts are the secondary object, then the Add Fields Via Lookup overlay doesn't display lookup fields from contacts to accounts.
 - Fields added to the layout via the **Add fields related via lookup** link are automatically included in the section of the object from which they're a lookup field. For example, if you add the `Contact` field as a lookup from accounts, then the `Contact` field is automatically included in the Accounts section. However, you can drag a field to any section.
 - You can add up to 1000 fields to each custom report type. A counter at the top of the Page Layout step shows the current number of fields. If you have more than 1000 fields, you can't save the layout.
 - Fields added via lookup automatically display the lookup icon on the field layout of the custom report type.
 - Reduce the amount of time it takes to find fields in a report by grouping similar fields together on custom report type field layouts. You can create page sections in which to group fields that are related to one another, and you can group fields to match specific detail pages and record types.
 - If you include Activities as the primary object on a custom report type, you can only add lookup fields from Activities to Account on the select column layout of the custom report type.
-  **Note:** Custom fields that you add to a Salesforce object are added automatically to all the custom report types based on that object. When you create a report from the custom report type, all the custom fields are available for you to add to your report.

Manage Custom Report Types

After you create a custom report type, you can customize, edit, and delete it.

Start by displaying the list of custom report types for your organization. From Setup, enter *Report Types* in the *Quick Find* box, then select **Report Types**. If the Custom Report Type welcome page opens, click **Continue**.

- Select a list view from the *View* dropdown list. To define your own custom list view, click **Create New View**.
- Define a new custom report type by clicking **New Custom Report Type**.
- Update a custom report type's name, description, report type category, and deployment status by clicking **Edit** next to a custom report type's name.
- Delete a custom report type by clicking **Del** next to the custom report type's name. All the data stored in the custom report type is deleted and can't be restored from the Recycle Bin.

 **Important:** When you delete a custom report type, any reports based on it are also deleted. Any dashboard components created from a report based on a deleted custom report type display an error message when viewed.

- Display detailed information about a custom report type and customize it further by clicking a custom report type's name.

After you click a custom report type name you can:

- Update which object relationships a report can display when run from the custom report type.
- Specify the standard and custom fields a report can display from the custom report type by editing the page layout.
- See how the fields display to users in reports run from the custom report type by clicking **Preview Layout** on the Fields Available for Reportings.
- Create a custom report type with the same object relationships and fields as the selected custom report type by clicking **Clone**.
- Rename fields in the report.
- Set which fields are selected by default.

In Lightning Experience, the report type is displayed on the report run page in the upper left area near the report name. In Salesforce Classic, the report type is displayed in the report builder near the report name.

 **Note:** If the Translation Workbench is enabled for your organization, you can translate custom report types for international users.

Limits on Report Types

Custom report types are subject to some limits for high performance and usability.

- A custom report type can contain up to 60 object references. For example, if you select the maximum limit of four object relationships for a report type, you can select fields via lookup from an extra 56 objects.
- If a user runs a report from a custom report type and the report has columns from more than 20 different objects, an error occurs.
- You can add up to 1,000 fields to each custom report type. A counter at the top of the Page Layout step shows the current number of fields. If you have too many fields, you can't save the layout.
- You can't add these fields to custom report types:
 - Product schedule fields

EDITIONS

Available in: Salesforce Classic (**not available in all orgs**) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

Available in: Enhanced Folder Sharing and Legacy Folder Sharing

USER PERMISSIONS

To create and update custom report types:

- Manage Custom Report Types

To delete custom report types:

- Modify All Data

- History fields
- The `Age` field on cases and opportunities
- Lookup fields on the Opportunity Team Member object
- Custom report types based on the Service Appointments object don't support these fields:
 - Parent Record
 - Owner
- Object references can be used as the main four objects, as sources of fields via lookup, or as objects used to traverse relationships. Each referenced object counts toward the maximum limit even if no fields are chosen from it. For example, if you do a lookup from account to account owner's role, but select no fields from account owner, all the referenced objects still count toward the limit of 60.
- Reports run from custom report types that include cases don't display the Units dropdown list, which lets users view the time values of certain case fields by hours, minutes, or days.
- Report types associated with custom objects in the Deleted Custom Objects list count against the maximum number of custom report types you can create.
- Reports on feed activities don't include information about system-generated posts, such as feed tracked changes.
- Custom report type names support up to 50 characters. If you enter a name that is longer than 50 characters, the name gets truncated.
- Custom report type descriptions support up to 255 characters. If you enter a name that is longer than 255 characters, the name gets truncated.
- When a lookup relationship is created for a standard or custom object as an Opportunity Product field, and then a custom report type is created with that primary object, Opportunity Product isn't available as a secondary object for that custom report type.

Bulk Move Reports or Dashboards with Metadata API

You can move reports or dashboards between folders and subfolders in Lightning Experience. If you want to move reports or dashboards in bulk, use Metadata API.

For example, the Some Old Deprecated Folder folder contains two reports: My Accounts Report and My Opty Report. You want to move My Accounts Report to a new folder called Accounts and My Opty Report to the new Opportunities folder.

Reports	
ALL FOLDERS > SOME OLD DEPRECATED FOLDER	
2 items	
REPORTS	NAME
Recent	My Accounts Report
Created by Me	My Opty Report
Private Reports	

This example uses Reports and Dashboards REST API to get the details of the reports that you want to move and Metadata API to move the reports. (The same process works for dashboards.) You can use Postman or cURL to call Reports and Dashboards REST API. You can use Salesforce Extensions for Visual Studio Code or Salesforce CLI to execute Metadata API. You can follow a similar process using the force.com ANT migration tool.

1. Get a list of your reports using the Reports and Dashboards REST API [report resource PATCH method](#).
2. Search the list to get the developer names of the reports you want to move and the ID of the folder they are in.
3. Use the folder ID to obtain the folder's developer name with the [folder operation GET method](#).

4. Create a `package.xml` manifest using the folder and file developer names as members.

```
<?xml version="1.0" encoding="UTF-8"?>
<Package xmlns="http://soap.sforce.com/2006/04/metadata">
  <types>
    <name>Report</name>
    <members>Some_Old_Deprecated_Folder/My_Accounts_Report_eQ</members>
    <members>Some_Old_Deprecated_Folder/My_Opty_Report_CO</members>
  </types> <version>43.0</version>
</Package>
```

5. Retrieve a package that contains the reports using the Metadata API `retrieve()` call.
6. Unzip the package.

Folder/Files	Time	Size	Type
unpackaged	Today, 3:08 PM	--	Folder
package.xml	Today, 11:07 PM	337 bytes	XML
reports	Today, 3:08 PM	--	Folder
Some_Old_Deprecated_Folder	Today, 3:08 PM	--	Folder
My_Accounts_Report_eQ.report	Today, 11:07 PM	903 bytes	Document
My_Opty_Report_CO.report	Today, 11:07 PM	2 KB	Document

7. In the unzipped package, create the new folder and file structure.

Folder/Files	Time	Size	Type
unpackaged	Today, 3:08 PM	--	Folder
package.xml	Today, 11:07 PM	337 bytes	XML
reports	Today, 3:12 PM	--	Folder
Accounts	Today, 3:11 PM	--	Folder
My_Accounts_Report_eQ.report	Today, 11:07 PM	903 bytes	Document
Opportunities	Today, 3:11 PM	--	Folder
My_Opty_Report_CO.report	Today, 11:07 PM	2 KB	Document

8. In the `package.xml` file manifest, change the folder structure to match the changes that you made in the unzipped package.

```
<?xml version="1.0" encoding="UTF-8"?>
<Package xmlns="http://soap.sforce.com/2006/04/metadata">
  <types>
    <members>Accounts/My_Accounts_Report_eQ</members>
    <members>Opportunities/My_Opty_Report_CO</members>
    <name>Report</name>
  </types>
  <version>43.0</version>
</Package>
```

9. Create the new folders in Lightning Experience.

Reports	
ALL FOLDERS	
3 items	
REPORTS	NAME
Recent	Accounts
Created by Me	Opportunities
Private Reports	Some Old Deprecated Folder
Public Reports	

10. Create the package for deployment.

This command creates a ZIP file from the contents of the unzipped package directory called `unpackaged`.

```
zip -r move_reports.zip unpackaged/
```

11. Deploy the package that contains the moved reports using the Metadata API `deploy()` call.

The move is complete. Some Old Deprecated Folder is empty, and you can delete it in the UI.

SEE ALSO:

[Deploying and Retrieving Metadata \(Metadata API Developer Guide\)](#)

Set Up Historical Trend Reporting

Historical trend reporting allows you to track how field values have changed over time.

User Permissions Needed

To create, edit, and delete reports in private folders:	Create and Customize Reports
---	------------------------------

To create, edit, and delete reports in public and private folders:	Report Builder
--	----------------

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise, Performance, Unlimited, and Developer** Editions

Available in: Enhanced Folder Sharing

When setting up historical trend reporting, keep in mind that retaining historical data increases storage requirements. For effective historical reports, you need enough data for meaningful results but not so much that you risk exceeding space limits. Consider which fields contain useful historical data and which you can omit.

The effect of historical reporting on amount of data depends on the way your organization works. For example, historical trending data for the Status field on the Opportunity object takes up more space if the record changes one time per week vs one time per month.

 **Note:** If any of your trended objects is in danger of exceeding the data limit, your organization administrator receives an email alert.

 **Note:** Historical trend reports are also called historical tracking reports.

1. From Setup, enter *Historical Trending* in the Quick Find box, then select **Historical Trending**.
2. Select the object that you want to do historical trend reporting on.
You can select Opportunities, Cases, Forecasting Items, and up to 3 custom objects.

3. Select `Enable Historical Trending`.**4. To narrow down the amount of data that's captured for historical trend reporting, use the filters under `Configure Data`.**

You can narrow down historical data for Opportunities, Cases, and custom objects. For Forecasting Items, the available data is selected for you.

For example, to reduce the data stored for Opportunities reports, you can forego historical tracking on deals that aren't active opportunities by setting `Stage not equal to Closed`.

5. Under `Select Fields`, choose up to 8 fields to make available for historical trend reporting. For Opportunities reporting, 5 fields are preselected: Amount, Close Date, Forecast Category, Probability, and Stage. You can add 3 more. For Forecasting, all 8 available fields are pre-selected.**6. Click `Save`.**

After you enable historical trending, a new report type is available when you create future reports. For example, if Opportunities is enabled for historical trending, a new report called "Opportunities with Historical Trending" is available when you create a report. If you enable historical trending on a new field, that field is automatically added to the historical trending report layout.

For opportunities, historical data is collected even if historical trending isn't enabled. If historical trending is enabled, the historical reports include all the data for the specified time range, including data from prior to when historical trending was enabled. The collection is subject to data limits for historical trend reporting.

When you turn off historical trending, keep these points in mind.

- In Developer Edition orgs, you can't turn off historical trending on a custom field that is part of a released managed package. This is to avoid issues that arise during subsequent installations of the package. To turn off tracking on a custom field that is part of an unreleased version of a managed package in a Developer Edition org, contact Salesforce support.
- Turning off historical trending for a field hides the historical data for that field. If you re-enable historical trending, historical data for the field can be viewed again, including data created after historical trending was turned off.
- Turning off historical trending for an object causes all historical data and configuration settings to be deleted for that object. The object's historical trending report type and any reports that have been created with it are also deleted.
- If you turn off historical trending for a field and delete it, the field's historical data is no longer available even if you re-enable historical trending.

**Note:**

- The historical fields available to each user depend on the fields that user can access. If your permissions change and you can no longer see a given field, that field's historical data also becomes invisible.
- Each historical field has the same field-level security as its parent field. If the field permissions for the parent field change, the historical field's permissions change accordingly.

Upgrade the Report Wizard

Report builder, a powerful drag-and-drop editor, is the standard tool for creating and editing reports. If your organization is still using the old report wizard, you should upgrade to report builder.

- All profiles get access to the report builder by default. (You may continue to see the "Report Builder" permission in permission sets and profiles and the PermissionSet and Profile objects in the API, though the upgrade overrides those settings.)
- The old report wizard is available only to users in Accessibility Mode.
- Group and Professional Edition organizations can use report builder.
- You get scatter charts, a new chart type for reports.

USER PERMISSIONS

To modify report and dashboard settings:

- `Customize Application`

Assigning the “Report Builder” permission or the “Report Builder (Lightning Experience)” permission to all users through profiles or permission sets isn’t the same thing as enabling report builder for your entire organization.

New organizations automatically get the latest version of report builder. If you don’t see the Report Builder Upgrade section on the User Interface Settings page, the upgrade has already been enabled for your organization.

1. From Setup, enter *Reports* in the *Quick Find* box, then select **Reports and Dashboards Settings**.
2. Check **Enable Lightning Report Builder (Beta)**.
3. Review the Report Builder Upgrade section of the page and click **Enable**. If you don’t see the button, report builder has already been enabled for your entire organization.
4. Confirm your choice by clicking **Yes, Enable Report Builder for All Users**.
5. Click **Save**.

Important: Upgrading **does not affect** any of your existing reports. However, once you upgrade, you can’t return to the old report wizard.

Release Updates

Salesforce periodically releases updates that improve the performance, security, logic, and usability of your Salesforce org, but that can affect your existing customizations. When these updates become available, Salesforce shows them in the Release Updates node in Setup.

Release updates offer a more detailed view of information previously found in the Critical Updates console. The page also contains information previously found in the Security Alerts node.

EDITIONS

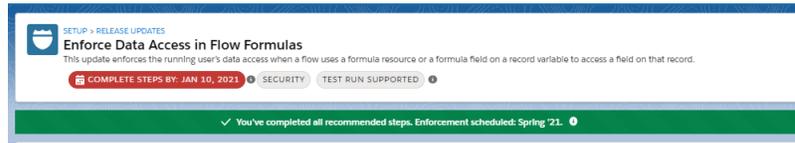
Available in: both Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: all editions

The screenshot shows the 'Release Updates' page in Salesforce Setup. At the top, there are tabs for 'NEEDS ACTION', 'DUE SOON', 'OVERDUE', and 'ARCHIVED'. The 'NEEDS ACTION' tab is active. Below the tabs, there are four update cards, each with a title, a progress bar, and a 'Get Started' button. The cards are: 1. 'Enable Secure Static Resources for Lightning Components' (Security, 0% complete, due Nov 29, 2020). 2. 'Prevent consecutive API navigation calls in Visualforce pages' (Usability, 0% complete, due Jan 10, 2021). 3. 'Enforce Data Access in Flow Formulas' (Security, 0% complete, due Jan 10, 2021). 4. 'Require Permission to View Record Names in Lookup Fields' (Security, 0% complete, due Jan 10, 2021). Each card also has a 'View Details' link and an 'Enforcement Scheduled' date.

- Use tabs to view release updates for a specific category.
 - Needs Action: Update hasn’t reached the Complete Steps By date and steps aren’t done.
 - Due Soon: Complete Steps By date is approaching.
 - Overdue: Update is past the Complete Steps By date and steps aren’t done.
 - Archived: Update is completed.

When you view updates in **Due Soon**, **Overdue**, or **Archived**, a banner appears at the top indicating the status of the update. For example, a completed update in **Archived** shows: You've completed all recommended steps, and includes enforcement information.



Note: In Beta, the text Due Soon appeared at the top of the detail page for updates with upcoming enforcement dates. This text no longer appears on the detail page.

- Check the Complete Steps By date. The test run button is a toggle that you can enable and disable before this date (sandbox org test periods may end earlier). When you enable a test run, the update becomes immediately enabled in your org. The test run allows you to evaluate the impact of the update before the update is enforced.
- Use the Enforcement Scheduled or Enforced In information to check the release in which Salesforce enforces the update. In the Beta release, we indicated the enforcement information with Automatically enforced in. To find out where to get the major release upgrade date for your instance, hover over the tooltip.

Note: Some release updates contain specific dates. In these cases, use the date information in the update as guidance for when to expect enforcement.

- Get quick information about an update without leaving the home page by clicking **View Details**.
- Start or stop a test run, complete update steps, and view step update history by clicking **Get Started**.

When you act on an update, a series of detailed steps helps you to evaluate the impact on your org. You can adopt the update early or, depending on your org, use the recommended test run option.

[Manage Release Updates](#)

Act on release updates to keep your Salesforce org functioning at its best. Release updates replace the Critical Updates console and include more detailed information about upcoming changes.

[Security Alerts](#)

Release updates have replaced security alerts. Information about previously released security alerts can be found in the Release Updates node.

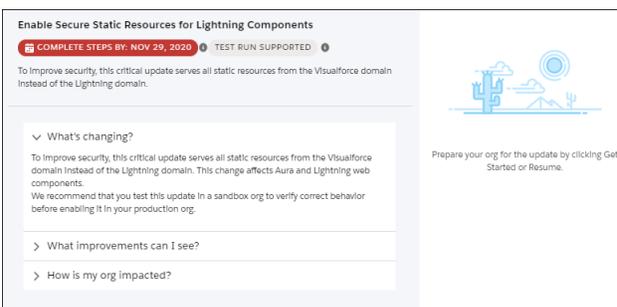
Manage Release Updates

Act on release updates to keep your Salesforce org functioning at its best. Release updates replace the Critical Updates console and include more detailed information about upcoming changes.

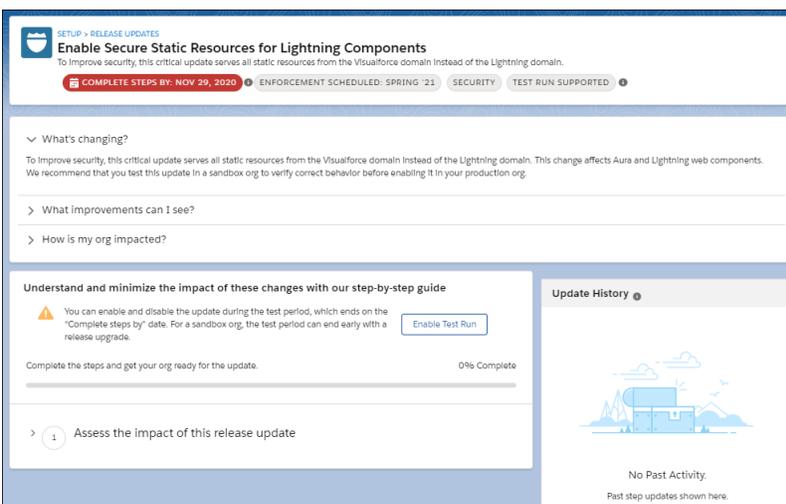
The Release Updates page provides a list of updates that affect your org. Each update includes step-by-step actions for you to take. To ensure a smooth transition, many release updates have test runs available. Use the test run option to activate or deactivate an update before the Complete Steps By date so that you can evaluate its impact on your org.

 **Warning:** Salesforce recommends testing each update by activating it in either your developer sandbox or your production environment during off-peak hours.

1. From Setup, in the Quick Find box, enter *Release Updates*, and then select **Release Updates**.
2. On the Release Updates page, select an update.
3. Get quick information about an update without leaving the home page by clicking **View Details**. Use the expandable sections to see details about the changes, improvements you can expect, and impact on your org.



4. Click **Get Started** to act on your update. From this page, you can enable a test run if it's available for your update, and review the specific steps to take.



EDITIONS

Available in: both Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: all editions

USER PERMISSIONS

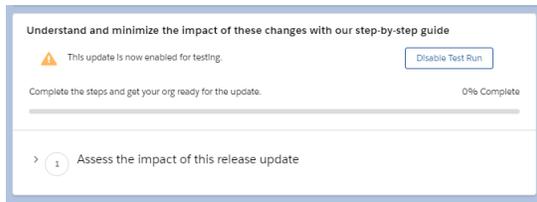
To view release updates:

- View Setup and Configuration

To enable or disable release updates:

- Manage Release Updates OR Customize Application

- a. If you enabled a test run and find in testing that you must disable the update, click **Disable Test Run**. You can enable or disable test runs as often as needed until the Complete Steps By date on your update. On sandbox orgs, the test run periods can end earlier than the Complete Steps By date.



5. After you finish the steps, click **Done**.
6. Confirm that you reviewed and completed the update steps.

Final Confirmation

After confirmation, the steps cannot be changed.

I have reviewed the steps and understand the impact of this update on my org.

I have completed necessary testing of this update for my org.

Cancel
Confirm

SEE ALSO:

[Release Updates](#)

Security Alerts

Release updates have replaced security alerts. Information about previously released security alerts can be found in the Release Updates node.

SEE ALSO:

[Release Updates](#)

Organize Data with Divisions

Divisions let you segment your organization's data into logical sections, making searches, reports, and list views more meaningful to users. Divisions are useful for organizations with extremely large amounts of data.

Divisions do not restrict access to data and are not meant for security purposes.

[How Divisions Work](#)

Divisions can be assigned to users and other kinds of records. For example, you can create a report to show the opportunities for just the North American division to get accurate sales numbers for the North American sales team.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

[Set Up Divisions](#)

When setting up divisions, you must create divisions and assign records to divisions to make sure that your data is categorized effectively.

[Create and Edit Divisions](#)

Creating logical divisions for your organization helps you segment your records to make searching and reporting easier.

[Transferring Multiple Records Between Divisions](#)

Select groups of records to move into or between divisions.

[Change the Default Division for Users](#)

If you can manage user settings, you can change a user's default division.

[Reporting With Divisions](#)

If your organization uses divisions to segment data, you can customize your reports to show records within specific divisions.

How Divisions Work

Divisions can be assigned to users and other kinds of records. For example, you can create a report to show the opportunities for just the North American division to get accurate sales numbers for the North American sales team.

-  **Important:** Where possible, we changed noninclusive terms to align with our company value of Equality. We maintained certain terms to avoid any effect on customer implementations.
- Record-level division—Division is a field on individual records that marks the record as belonging to a particular division. A record can belong to a division created by the administrator or the standard “global” division. The standard global division is created automatically when your organization enables divisions. A record can belong to only one division at a time.
 - Default division—Users are assigned a default division that applies to their newly created accounts, leads, and custom objects that are enabled for divisions.
 - Working division—If you have the “Affected by Divisions” permission, you can set the division using a drop-down list in the sidebar. Then, searches show only the data for the current working division. You can change your working division at any time. If you don't have the “Affected by Divisions” permission, you always see records in all divisions.

The following table shows how using divisions affects different areas.

Area	Description
Search	<p>If you have the “Affected by Divisions” permission:</p> <ul style="list-style-type: none"> In sidebar search, you can select a single division, or all divisions. In advanced search, you can select a single division or all divisions. In global search, you can search a single division or all divisions. For searches in lookup dialogs, the results include records in the division you select from the drop-down list in the lookup dialog window. <p>All searches within a specific division also include the global division. For example, if you search within a division called Western</p>

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer Editions**

Area	Description
List views	<p>Division, your results include records found in both the Western Division and the global division.</p> <p>If you do not have the “Affected by Divisions” permission, your search results always include records in all divisions.</p>
Chatter	<p>Chatter doesn’t support divisions. For example, you can’t use separate Chatter feeds for different divisions.</p>
Reports	<p>If you have the “Affected by Divisions” permission, you can set your report options to include records in just one division or all divisions. Reports that use standard filters (such as My Cases or My team’s accounts) show records in all divisions, and can’t further limited to a specific division.</p> <p>If you do not have the “Affected by Divisions” permission, your reports always include records in all divisions.</p>
Viewing records and related lists	<p>When viewing the detail page of a record, the related lists show all associated records that you have access to, regardless of division.</p>
Creating records	<p>When you create accounts, leads, or custom objects that are enabled for divisions, the division is automatically set to your default division, unless you override this setting.</p> <p>When you create records related to an account or other record that already has a division, the new record is assigned to the existing record’s division. For example, if you create a custom object record that is on the detail side of a master-detail relationship with a custom object that has divisions enabled, it is assigned the master record’s division.</p> <p>When you create records that are not related to other records, such as private opportunities or contacts not related to an account, the division is automatically set to the global division.</p>
Editing records	<p>When editing accounts, leads, or custom objects that are enabled for divisions, you can change the division. All records that are associated through a master-detail relationship are automatically transferred to the new division as well. For example, contacts and opportunities are transferred to the new division of their associated account. Detail custom objects are transferred to their master record’s new division.</p>

Area	Description
Custom objects	<p>When editing other types of records, you can't change the division setting.</p> <p>When you enable divisions for a custom object, Salesforce initially assigns each record for that custom object to the global division.</p> <p>When you create a custom object record:</p> <ul style="list-style-type: none"> • If the custom object is enabled for divisions, the record adopts your default division. • If the custom object is on the detail side of a master-detail relationship with a divisions-enabled custom object, the record adopts the division of the master record.
Relationships	<p>If you convert a lookup relationship to a master-detail relationship, detail records lose their current division and inherit the division of their master record.</p> <p>If you convert a master-detail relationship to a lookup relationship, the previous master record determines the division for any detail records.</p> <p>If you delete a master-detail relationship, the previous master record determines the division for any detail records.</p>

Set Up Divisions

When setting up divisions, you must create divisions and assign records to divisions to make sure that your data is categorized effectively.

Before you can use the divisions feature for your organization, you must enable divisions. If you are using a standard object, contact Salesforce to enable divisions for your organization. For custom objects, select **Enable Divisions** on the custom object definition page to enable divisions.

1. Plan which divisions you need based on how you want to segment your data.
For example, use one division for all the records belonging to your North American sales team and one division for your European sales team.
100
2. [Create divisions](#) for your organization. All existing records are assigned to the "Global" division by default. You can change the default division name, create more divisions, and move user and data records between divisions.
3. [Transfer leads, accounts, and custom objects into relevant divisions](#). When records are assigned to a division, associated records are assigned the same division.
For example, when you change the division assigned to an account, related records such as contacts and opportunities are assigned to the same division.
4. Add division fields to page layouts.
5. Add divisions to field-level security.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To create or edit divisions:

- [Modify All Data](#)

6. Set the default division for all users. New accounts and leads are assigned to the user's default division unless the user explicitly assigns a different division. New records related to existing records are assigned to the existing record's division.
7. Enable the "Affected by Divisions" permission for users.
Users with this permission can limit list views by division, search within a division, or report within a division. Users who don't have the "Affected by Divisions" permission still have a default user-level division. They can view division fields, change the division for a record, and specify a division when creating records.

Create and Edit Divisions

Creating logical divisions for your organization helps you segment your records to make searching and reporting easier.

Divisions must be enabled for the organization.

All records are initially assigned to the default "Global" division until the user defines the division. You can create up to 100 divisions, including any inactive ones.

1. From Setup, enter *Manage Divisions* in the Quick Find box, then select **Manage Divisions**.
2. To create a division, click **New**, or **Edit** change an existing division.
3. Enter the division name.
4. To make the division active, select the checkbox.

 **Note:** You can't deactivate a division if users or lead queues are assigned to that division.

5. Click **Save**.
6. To change the order that divisions appear in the Divisions picklist, click **Sort**. Then to use the arrow buttons to move divisions higher or lower in the list.

Transferring Multiple Records Between Divisions

Select groups of records to move into or between divisions.

To reassign the divisions for multiple records at one time, transfer groups of accounts, leads, or users between divisions.

1. From Setup, enter *Mass Division Transfer* in the Quick Find box, then select **Mass Division Transfer**.
2. Select the type of record you want transferred, then click **Next**. When you change the division assigned to an account, related records such as contacts and opportunities are assigned to the same division. When you change the division assigned to a custom object, other custom objects belonging to it are also transferred to the new division.
3. Select search conditions that records must match and click **Next**.
4. Select the division you want to transfer the records to.
5. If you're transferring user records, you can select *Change the division...* to also transfer the users' records to the new division.
6. Click **Transfer**. You'll receive an email notification when the transfer is complete. If 5,000 or more records are being transferred, the request will be placed in a queue for processing.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To create or edit divisions:

- **Modify All Data**

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To mass transfer records:

- **Modify All Data**

Change the Default Division for Users

If you can manage user settings, you can change a user's default division.

If your organization uses divisions to segment data, a default division is assigned to all users and is applied to new accounts, leads, and appropriate custom objects. The default division doesn't prevent users from viewing or creating records in other divisions. If, however, the new record is related to an existing record, the new record is assigned the same division as the existing record.

1. From Setup, enter *Users* in the **Quick Find** box, then select **Users**.
2. Click the name, alias, or username of the user whose default division you want to change.
3. Next to the **Default Division** field, click **Change**.
4. Select a new default division.
5. Select an action to be applied to records the user already owns.
6. Click **Save**.

If you are changing your own default division, skip step 1 and go to your personal settings. Enter *Advanced User Details* in the **Quick Find** box, then select **Advanced User Details**. No results? Enter *Personal Information* in the **Quick Find** box, then select **Personal Information**.

Reporting With Divisions

If your organization uses divisions to segment data, you can customize your reports to show records within specific divisions.

Use the **Division** drop-down list on the report to select one of the following.

- A specific division
- Your current working division.
- All records across all divisions.

 **Note:** Reports that use standard filters (such as *My Cases* or *My Team's Accounts*) show records in all divisions. These reports can't be further limited to a specific division.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To change a user's default division:

- [Manage Users](#)

USER PERMISSIONS

To create, edit, and delete reports:

- **Legacy Folder Sharing**
Create and Customize Reports
AND
Report Builder
- **Enhanced Folder Sharing**
Create and Customize Reports
AND
Report Builder

Salesforce Upgrades and Maintenance

Salesforce reserves up to five minutes of service interruption for major upgrades, but you have access your data during other maintenance events, like splits and migrations.

Read-Only Mode

Access to your data at a moment's notice—even during our planned maintenance windows. To minimize interruption to your business, Salesforce gives users read-only access during splits, instance migrations, instance switches, pre-scripts, and certain other maintenance events.

5 Minute Upgrades

Salesforce reserves just five minutes of scheduled maintenance time to roll out new major versions of our service. These upgrades to the next release occur three times per year.

Check for Desktop Client Updates

Desktop clients such as Salesforce for Outlook and Connect Offline integrate Salesforce with your PC. Your administrator controls which desktop clients you are allowed to install.

Read-Only Mode

Access to your data at a moment's notice—even during our planned maintenance windows. To minimize interruption to your business, Salesforce gives users read-only access during splits, instance migrations, instance switches, pre-scripts, and certain other maintenance events.

EDITIONS

Available in: **All Editions**

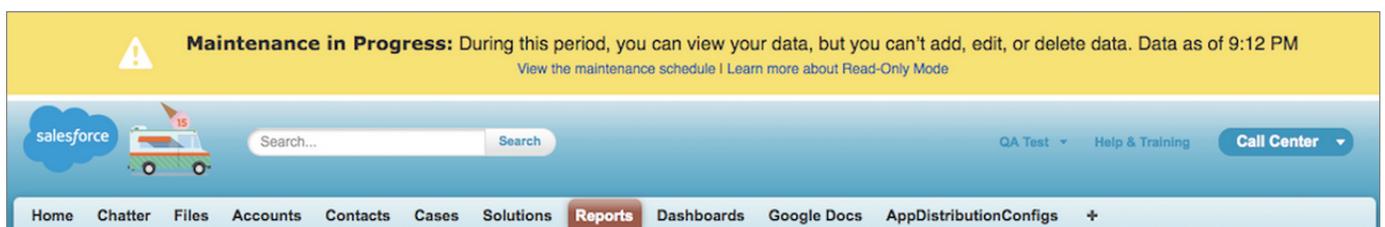
What to Expect in Read-Only Mode

When Salesforce is in read-only mode, you can navigate within the application and view and report on your business data. Activity reminders don't occur, and Recent Items lists don't update. Login history is still recorded for compliance purposes, but it isn't reflected in your organization until a few minutes after the organization exits read-only mode.

During read-only mode, you can't:

- Add, edit, or delete data
- Perform any actions in Salesforce that modify your Salesforce data. For example:
 - Post on Chatter
 - Use Chat
 - Refresh dashboards
 - Perform API write or edit actions
 - Perform bulk API read actions
 - Save new or edited reports
- Access the forecasts page (Collaborative Forecasts)

When your organization is in read-only mode, users see a banner at the top of their browser window:



When to Expect Read-Only Mode

The maintenance schedule posted on trust.salesforce.com indicates whether each upcoming maintenance window includes read-only access. Planned maintenance windows vary in length depending on the level of maintenance needed. In addition, when users are notified two weeks before a planned maintenance window, the notification specifies whether the maintenance includes read-only access.

If you'd like to see how your organization works in read-only mode, contact Salesforce to have the testing option enabled in your sandbox organization.

5 Minute Upgrades

Salesforce reserves just five minutes of scheduled maintenance time to roll out new major versions of our service. These upgrades to the next release occur three times per year.

Although your organization should expect to experience a disruption of up to five minutes, the interruption is typically one minute or less. Users receive an error message letting them know that the service is unavailable during the upgrade, and are prompted to log in again when the upgrade is complete.

Check for Desktop Client Updates

Desktop clients such as Salesforce for Outlook and Connect Offline integrate Salesforce with your PC. Your administrator controls which desktop clients you are allowed to install.

If your administrator enabled Home tab alerts, an alert banner displays on your Home tab when a new client version is available.

You can also see which clients are installed on your computer and check for updates on your own.

1. From your personal settings, enter *Check for Updates* in the **Quick Find** box, then select **Check for Updates**.
2. From the table, review the names and version numbers of available desktop clients.
3. If you are using Internet Explorer, click the correct desktop client and then click **Install Now** to install a client. If you are using another browser such as Mozilla Firefox, click **Download Now** to save the installer file to your computer. To run the installer program, double-click the saved file.

After you install the update, the alert banner displays on your Home tab until you log in through the newly updated client.

Permissions for UI Elements, Records, and Fields

To access UI elements, records or fields in Salesforce requires specific permissions. At a minimum, you must have the "Read" permission to view a tab, record, record field, related list, button, or link. To edit a record or record field, you must have the "Edit" permission.

What you can view or edit also depends on how you customized your personal display or page layout and what edition your org is using. This table described the different access levels in more detail.

Action	Access Needed
To view a tab:	You must have the "Read" permission on the records within that tab.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **All Editions**

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **All Editions** except for Database.com

USER PERMISSIONS

To view client update alerts:

- On, updates w/alerts
- OR
- On, must update w/alerts on your profile

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **All Editions** except **Database.com**

Action	Access Needed
To view a record:	<p>If you don't see a particular tab, verify that you customized your personal display to show the tab.</p> <p>You must have the "Read" permission on the type of record you want to view.</p> <p>If you can't view a certain record, check whether your org uses a sharing model or territory management. In certain sharing models, the owner of the record has to specifically share the record to grant view access to others. Territory management can restrict access to accounts, contacts, opportunities, and cases.</p>
To view a field:	<p>You must have the "Read" permission on the type of record for the field.</p> <p>If you can't view a certain field, check field-level security and your page layout. Field-level security can restrict access to a field. Page layouts can hide fields.</p>
To edit a field:	<p>You must have the "Edit" permission on the type of record for the field.</p> <p>If you can't edit a certain field, check field-level security and your page layout. Field-level security can restrict access to a field. Page layouts can set fields to not be editable.</p>
To view a related list:	<p>You must have the "Read" permission on the type of records displayed in the related list.</p> <p>If you can't view a certain field, check your page layout. Page layouts can hide fields.</p>
To view a button or link:	<p>Make sure that you have the necessary permission to perform the action. Buttons and links only display for users who have the appropriate user permissions to use them.</p>

Deactivate a Developer Edition Org

When a Developer Edition org has outlived its usefulness and it's time to move on, you can deactivate it or allow it to expire.

1. From Setup, in the Quick Find box, enter *Company Information*, and then select **Company Information**.
2. Click **Deactivate Org**.
3. Enter the org name to confirm its deactivation.
4. Click **Deactivate Org**.

If the org has released a managed package, you can't deactivate it. Contact Salesforce Customer Support for assistance.

Days after DE Org Deactivation	Can I Reactivate the Deactivated Org?
From 1 through 30	Yes. You can change your mind and reactivate the org via Setup.
From 31 through 60	Yes. The org is locked, but you can contact Salesforce Customer Support to reactivate the org.
From 61 and later	No. The org is permanently deleted and can't be reactivated.

EDITIONS

Available in: **Developer Edition**

USER PERMISSIONS

To view company information

- View Setup and Configuration

To deactivate an org

- Modify All Data

Developer Org Expiration

Developer edition (DE) orgs that haven't been logged into for 180 days are marked as inactive and queued for deletion.

Days after DE Org Flagged as Inactive	Can I Reactivate the Inactive Org?
From 1 through 14	Yes. Org admins receive an email about the pending org expiration. You can reactivate the org by logging in.
From 15 through 44	Yes. The org is locked, but you can contact Salesforce Customer Support to reactivate the org.
From 45 and later	No. The org is permanently deleted and can't be reactivated.

Some Developer Edition orgs are exempt from expiration.

- Orgs that have released a managed package. For example, packaging and patch orgs used in first-generation managed packaging, and Dev Hub orgs used in second-generation managed packaging.
- Orgs used to register a namespace.
- Orgs that have Environment Hub enabled.
- Orgs that are used for logging into Trailblazer or Partner Community.
- Salesforce Source Organizations.
- Orgs where a connected app was created. Note: Orgs where a connected app is installed are not exempt.

If your Developer Edition org expires, you can create a new DE org at <https://developer.salesforce.com>. Usernames associated with an expired DE org can be reused after the expired org has been deleted.

How Do I Discontinue Service?

If the service doesn't meet your needs, cancel it.

Users who are up to date with their payments can request a complete download of the data in the system.

To submit your request directly, contact the [Salesforce Customer Support Billing Department](#).

Manage Your Salesforce Account

Add products and licenses, manage your contracts and renewals, view and download invoices, and get account support right in your org with the Your Account app.

With Your Account app, you can:

- Increase your product and license count.
- Manage your contracts.
- Manage your renewals.
- Review and download invoices.
- Communicate with your account contact.

Manage your Salesforce account quickly and easily from within your Salesforce org.

Navigate to the Your Account app. Increase your product and license count in-app (1). Manage your contracts and renewals in-app (2). View and download invoices (3). Ask us for help (4). Give us feedback on the Your Account app (5).

EDITIONS

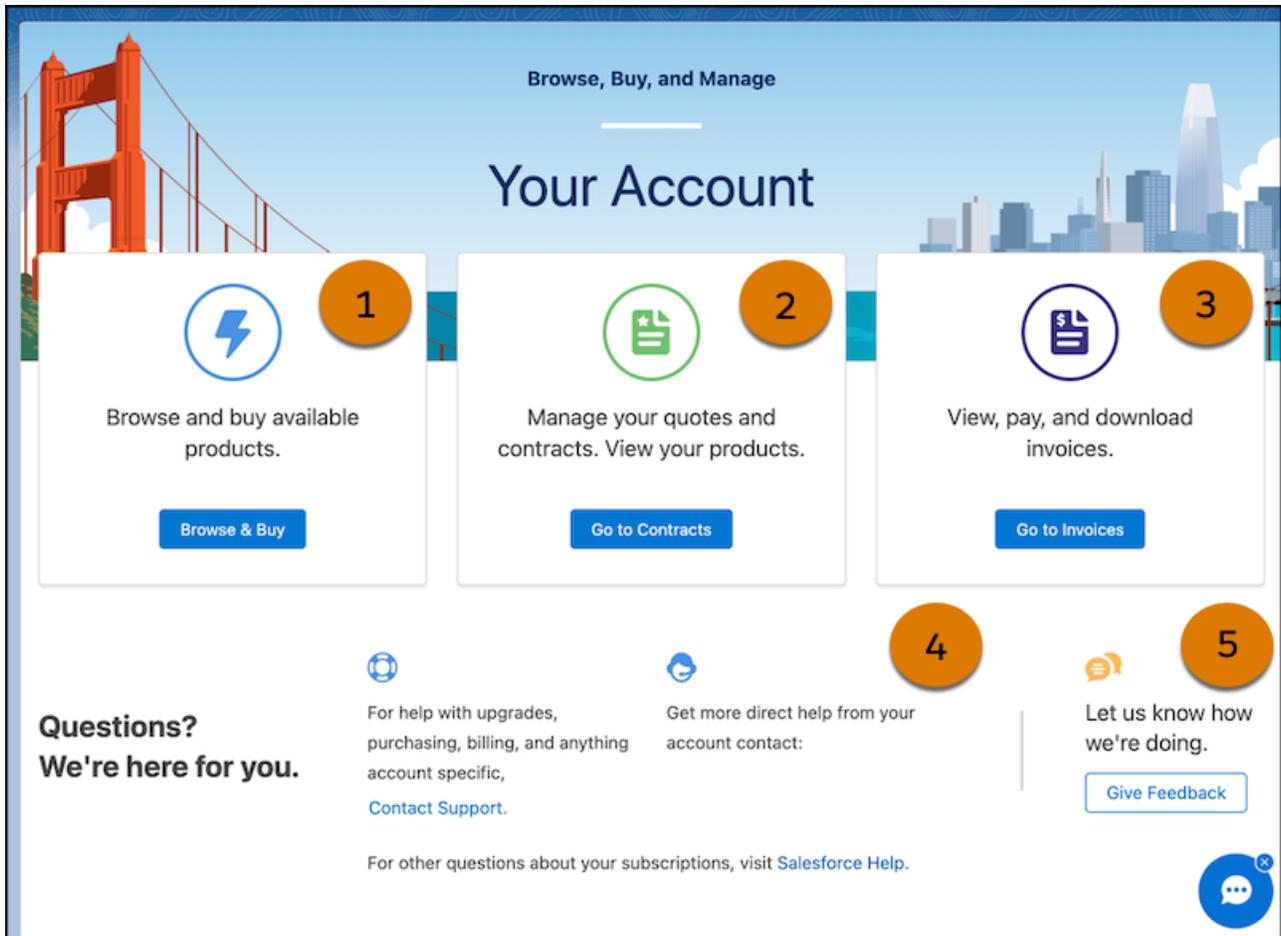
Available in: Salesforce Classic and Lightning Experience

Available in: **Starter**, **Professional**, **Enterprise**, **Performance**, and **Unlimited** Editions

USER PERMISSIONS

To use the Your Account app:

- Manage Billing or the Your Account App Admin User permission set



[Give Your Billing Users Free Access to the Your Account App](#)

Use Identity licenses to give your users access to the Your Account app if they don't need full access to Salesforce. The editions that support the Your Account app include 100 free Identity licenses that can be assigned as needed by the admin. Save your Salesforce licenses for the members of your team who need them.

[Launch the Your Account App](#)

Open the Your Account app from one of these areas depending on your edition.

[Add Products and Licenses with the Your Account App](#)

Purchase new products and licenses for your Salesforce org using the Your Account app. Products are pieces of Salesforce functionality, such as Sales Cloud, Sales Dialer, or extra file storage.

[Manage Your Contracts with the Your Account App](#)

See all your contracts in one place and request updates to your Salesforce org with the Your Account app. The keys to the ignition that keep your org running are just a few clicks away.

[Manage Renewals](#)

When your annual contract reaches 90 days before its renewal date, it's indicated on the Contracts and contract details pages. You can confirm the renewal, request changes, or choose not to renew. We can't accommodate cancellation requests until it's time to renew.

[View and Download Invoices](#)

In the Your Account app, you can review and download invoices and credit memos.

[Get Support with the Your Account App](#)

Ask product questions, manage billing, get technical support, and send us feedback, all from the Your Account app. Find these contact options on the app's home page.

[Turn Off the Your Account App](#)

Use the Your Account app to add products and licenses, manage your contracts and renewals, view invoices, and get account support right in Salesforce. You can turn it off for all your users, but we don't recommend it.

[Manage Your Quotes with the Your Account App](#)

You can manage quotes and complete your purchase using the new Pending Quotes tab on the updated Contract Details page. Review and sign, approve, and place your order using Your Account.

[Access Your Completed Quotes with the Your Account App](#)

You can review and download your completed quotes using the new Completed Quotes tab available on the updated Contract Details page in Your Account.

[Update Billing Contact Access to the Your Account App](#)

Make sure that the billing contact on each Salesforce contract has access to the Your Account app by granting access from the Contract page. When you give billing contacts access to Your Account, users get the permissions they must have to manage their billing and contracts.

SEE ALSO:

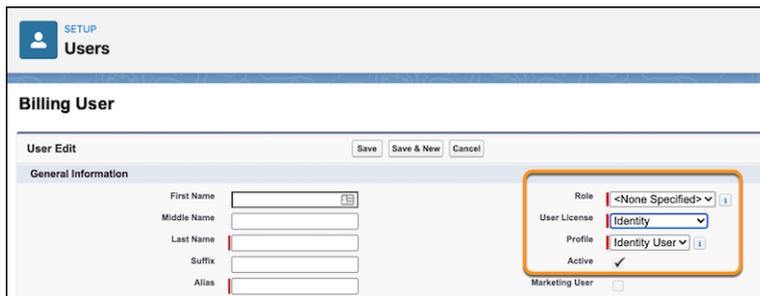
[User Permissions and Access](#)

Give Your Billing Users Free Access to the Your Account App

Use Identity licenses to give your users access to the Your Account app if they don't need full access to Salesforce. The editions that support the Your Account app include 100 free Identity licenses that can be assigned as needed by the admin. Save your Salesforce licenses for the members of your team who need them.

 **Note:** Admins and other Salesforce users with Manage Billing permission have access to the Your Account app and don't need the Your Account App Admin User permission set.

1. To provide free access to the Your Account app, create users with Identity licenses.
 - a. From Setup, in the Quick Find box, enter `users`, and then select **Users**.
 - b. Click **New User**, and then enter user information.
 - c. For **User License**, select **Identity**.



- d. Save the new user.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

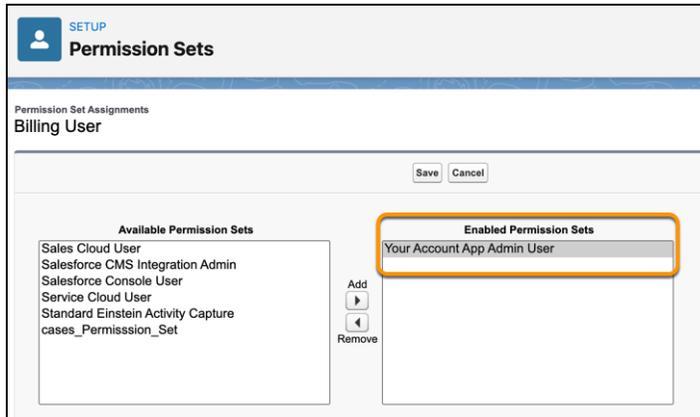
Available in: **Starter**, **Professional**, **Enterprise**, **Performance**, and **Unlimited** Editions

USER PERMISSIONS

To use the Your Account app:

- Manage Billing or the Your Account App Admin User permission set

2. Assign the Your Account App Admin User permission set to the Identity license users who need access to the Your Account app.
 - a. From Setup, in the Quick Find box, enter `users`, and then select **Users**.
 - b. Select the user, and then navigate to the **Permission Set Assignments** section and click **Edit Assignments**.
 - c. Select the **Your Account App Admin User** permission set and move it to Enabled Permission Sets. Then save the change.



SEE ALSO:

[Salesforce Help: Add a Single User](#)

[Salesforce Help: Manage Permission Set Assignments](#)

[Salesforce Help: Salesforce Identity Licenses](#)

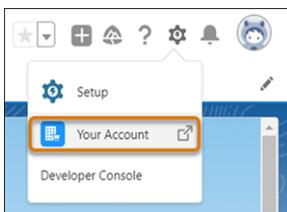
Launch the Your Account App

Open the Your Account app from one of these areas depending on your edition.

If you can't see the options described here, ask your admin for help.

In Professional, Enterprise, Performance, and Unlimited editions:

- Click **Setup** (⚙️) and then select **Your Account**



- Or from the App Launcher (☰), search for and select **Your Account**.

EDITIONS

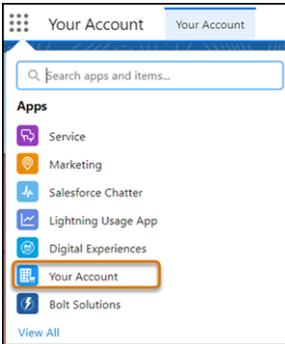
Available in: Salesforce Classic and Lightning Experience

Available in: **Starter**, **Professional**, **Enterprise**, **Performance**, and **Unlimited** Editions

USER PERMISSIONS

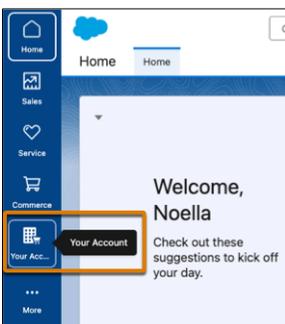
To use the Your Account app:

- Manage Billing or the Your Account App Admin User permission set

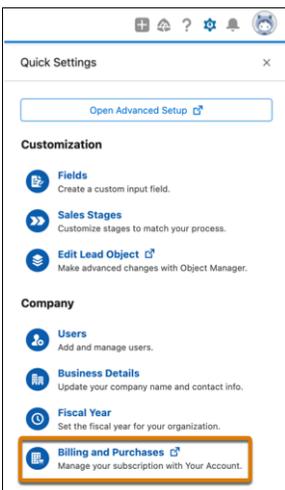


In Starter edition:

- From the menu on the left, select **Your Account**.



- Or from Quick Settings, click **Billing and Purchases**.

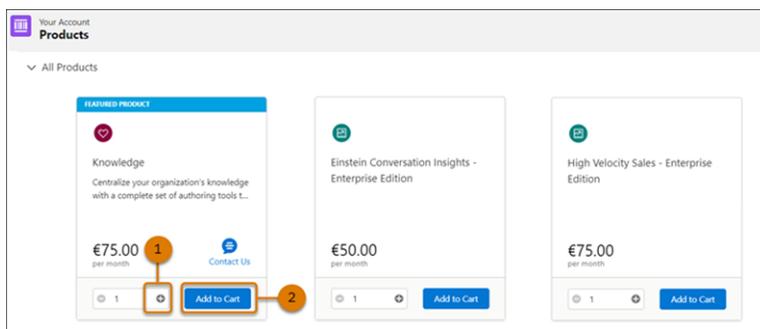


Add Products and Licenses with the Your Account App

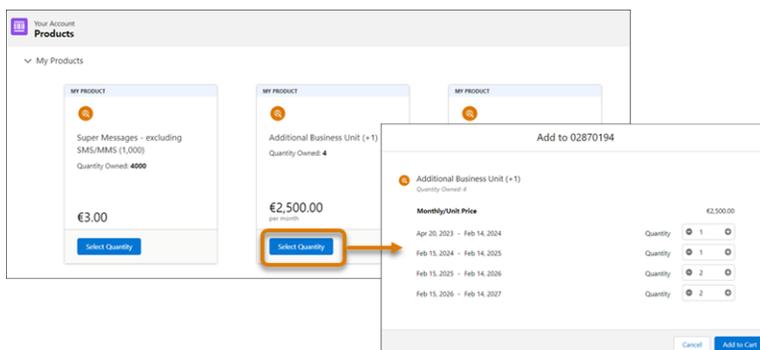
Purchase new products and licenses for your Salesforce org using the Your Account app. Products are pieces of Salesforce functionality, such as Sales Cloud, Sales Dialer, or extra file storage.

To purchase new products for your org:

1. Launch the [Your Account app](#).
2. Click **Browse & Buy**.
3. If you have multiple contracts, select the contract that you want to buy products or licenses for.
4. Click to expand the appropriate section of the page:
 - a. To buy new products, locate the All Products section, and find the product that you want to buy.
 - b. To buy additional quantities of products you own, locate the My Products section, and find the product that you want to add licenses for.
5. To specify the products that you want, select the quantity (1) and add to your cart (2).



For Marketing Cloud product subscriptions you own, you select the quantity in a popup. See the example that follows.



6. Open your cart.

EDITIONS

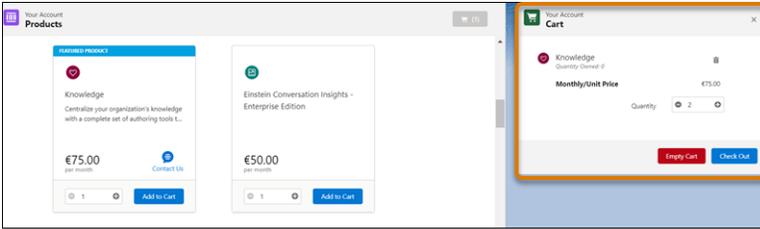
Available in: Salesforce Classic and Lightning Experience

Available in: **Starter**, **Professional**, **Enterprise**, **Performance**, and **Unlimited** Editions

USER PERMISSIONS

To use the Your Account app:

- Manage Billing or the Your Account App Admin User permission set



7. Review your order. Then click **Check Out**.
8. Review your payment and signature details:
 - a. If you pay by credit card, review your order total (before tax) and agree to the Subscription Agreement.
 - b. If you pay with a method other than a credit card, such as check, wire transfer, or direct debit, you don't have payment information to review. You also don't agree to a subscription agreement in this step.

 **Note:** If you're preparing a purchase that requires a different signer, you must use a payment method other than a credit card. You can [assign an approver to complete the process in DocuSign](#).
9. Use either of these steps to proceed:
 - a. If you pay by credit card, click **Place Order**.
 - b. If you pay with a method other than a credit card, click **Sign with DocuSign**, and check your email. To finalize your order, complete the steps in the email sent by DocuSign or [reassign to a different approver](#).
10. Your licenses are typically available within 45 minutes of purchase. To view your licenses:
 - a. From Setup, in the Quick Find box, enter *Company Information*, and then select **Company Information**.
 - b. See the User Licenses related list.
 - c. If you don't see your licenses after 45 minutes, contact Support.
11. To assign licenses to users:
 - a. From Setup, in the Quick Find box, enter *Users*, and then select **Users**.
 - b. Click **Edit** on the user's record, or click **New User**.
 - c. Select the license from the **User License** list.

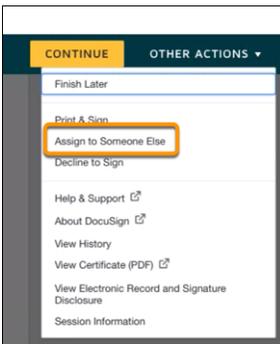
SEE ALSO:

[Get Support with the Your Account App](#)

Assign an Approver to Complete a Self-Service Quote with DocuSign

If you prepare a purchase but need someone else to sign for it, you can pass the documents to another person to complete the signing process.

1. [Launch the Your Account app](#).
2. [Add the products and licenses that you want to buy](#).
3. Click **Sign with DocuSign**.
4. Check your inbox for an email from DocuSign. To proceed in DocuSign, click the link in the email.
5. In DocuSign, click **Other Actions**. Then click **Assign to Someone Else**.



6. Enter the new signer's email address, name, and reason for changing the signing responsibility.
7. Click **ASSIGN TO SOMEONE ELSE**.

Your signer receives an email with a link to complete the signing process in DocuSign. When the signer completes the process, you both receive confirmation emails and your purchase is processed. For more information on what to expect and how to assign licenses to users, see [Add New Products and Licenses with the Your Account App](#).

 **Note:** This process is available only if your payment process isn't a credit card.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Starter, Professional, Enterprise, Performance, and Unlimited** Editions

USER PERMISSIONS

To use the Your Account app:

- Manage Billing or the Your Account App Admin User permission set

Manage Your Contracts with the Your Account App

See all your contracts in one place and request updates to your Salesforce org with the Your Account app. The keys to the ignition that keep your org running are just a few clicks away.

1. Launch the **Your Account** app.
2. Click **Go to Contracts**.
3. Select the contract that you want to review or update.

From the Contract Details page, you can manage your renewal. For annual subscriptions, click **Manage Renewal** (1). Add licenses and products (2). Edit payment information (3). Change the billing address or request to change the shipping address (4).

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Starter, Professional, Enterprise, Performance,** and **Unlimited** Editions

USER PERMISSIONS

To use the Your Account app:

- Manage Billing or the Your Account App Admin User permission set

Contract Details
Contract 01312161 Log Case

⚠ This contract will automatically renew soon.
Manage your renewal to make updates or contact us with questions. 1 [Manage Renewal](#)

Status: **Activated** | Billing Frequency: **Quarterly** | Starts On: **Feb 8, 2016** | Ends On: **Feb 7, 2024** | Auto-Renew: **On**

Product	Tenant ID	Current Quantity	Next Unit Price*	Actions
1 Additional API Calls - 10,000 per day	00DMK0000000839	0	\$25.00	Orders
2 Sales & Service Cloud - Enterprise Edition (Sales)	00DMK0000000839	24	\$9750	Orders Buy More
3 Salesforce Inbox - Enterprise Edition	00DMK0000000839	1	\$25.00	Orders Buy More

*Next Unit Price is the cost of the next product quantity you purchase, as determined by your contract. 2 [Add Products](#)

Payment Method 3
Payment Terms: **Net 30**
Payment Type: **Check**

Contact Details 4
Dispatch
BILLING ADDRESS
123 N. Washington Street
2nd Floor
Boston, MA 02114
US
[Edit](#)
Accounts Payable [Edit](#)
Billing Contact [ⓘ](#)
(877) 611-8768
marketing@salesforce.com/us/india

SEE ALSO:

[Salesforce Help: Manage Your Quotes with the Your Account App](#)

[Salesforce Help: Access Your Completed Quotes with the Your Account App](#)

Manage Renewals

When your annual contract reaches 90 days before its renewal date, it's indicated on the Contracts and contract details pages. You can confirm the renewal, request changes, or choose not to renew. We can't accommodate cancellation requests until it's time to renew.

The Time Remaining column in the Contracts page alerts you to your contract status and time remaining.

EDITIONS

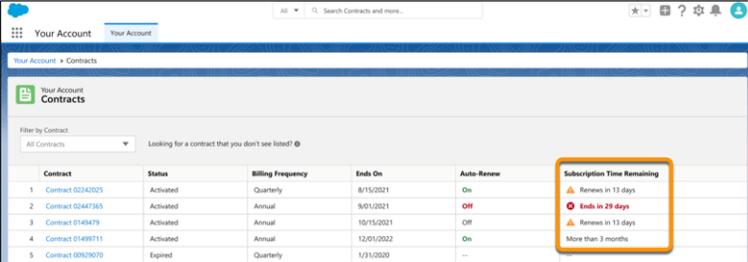
Available in: Salesforce Classic and Lightning Experience

Available in: **Starter**, **Professional**, **Enterprise**, **Performance**, and **Unlimited** Editions

USER PERMISSIONS

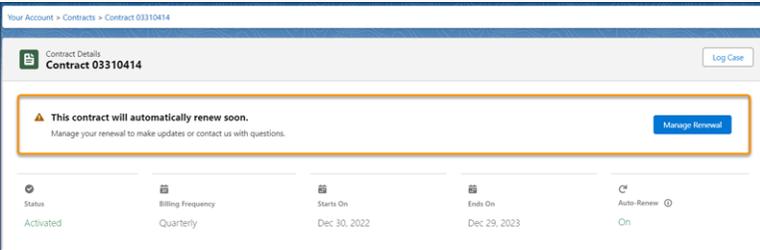
To use the Your Account app:

- Manage Billing or the Your Account App Admin User permission set



Contract	Status	Billing Frequency	Ends On	Auto-Renew	Subscription Time Remaining
1 Contract 0246825	Activated	Quarterly	8/15/2021	On	Renews in 13 days
2 Contract 02467365	Activated	Annual	8/01/2021	Off	Ends in 29 days
3 Contract 0149479	Activated	Annual	10/15/2021	Off	Renews in 13 days
4 Contract 01499711	Activated	Annual	12/01/2022	On	More than 3 months
5 Contract 08026076	Expired	Quarterly	1/31/2020	...	

When you view the contract details, a renewal status pane appears at the top of the Contract Details page. Save time and avoid interruption by reviewing your contract, requesting any changes, and confirming the automatic renewal.

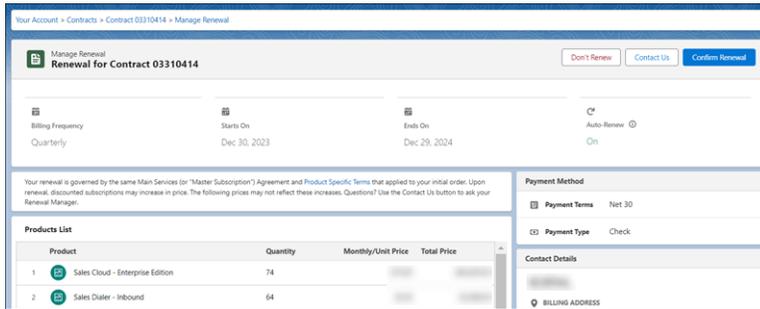


Status	Billing Frequency	Starts On	Ends On	Auto-Renew
Activated	Quarterly	Dec 30, 2022	Dec 29, 2023	On

 **Note:** Renewal management is unavailable in some cases. For help with your contract, check in with your Renewal Manager.

1. Launch the **Your Account** app.
2. Click **Go to Contracts**.
3. Select the contract that you want to review or update.

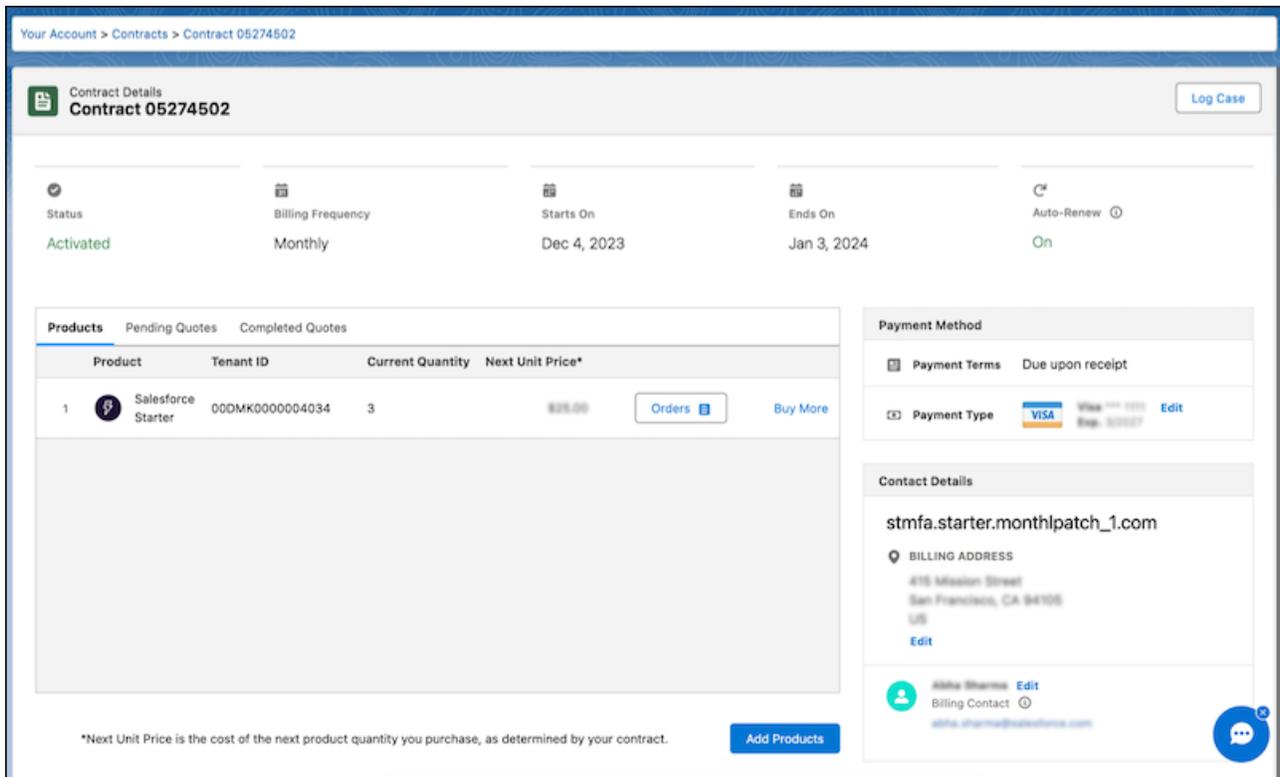
4. For an annual subscription, click **Manage Renewal**. Don't see the Manage Renewal button? It'll be there when your contract is within 90 days of renewal.



- To confirm your annual renewal, click **Confirm Renewal**.
- To request changes to your annual renewal, click **Contact Us** to submit a request to your Renewal Manager.
- To cancel an annual contract, click **Don't Renew**.

After you select an action, confirm that you're authorized to cancel, modify, and renew the contract to proceed.

If you have a monthly Starter subscription and you want to turn off automatic renewal, click **Log Case** on the Contract Details page. Select the Renewals option.



View and Download Invoices

In the Your Account app, you can review and download invoices and credit memos.

1. On the Your Account app home page, click **View Invoices**.

EDITIONS

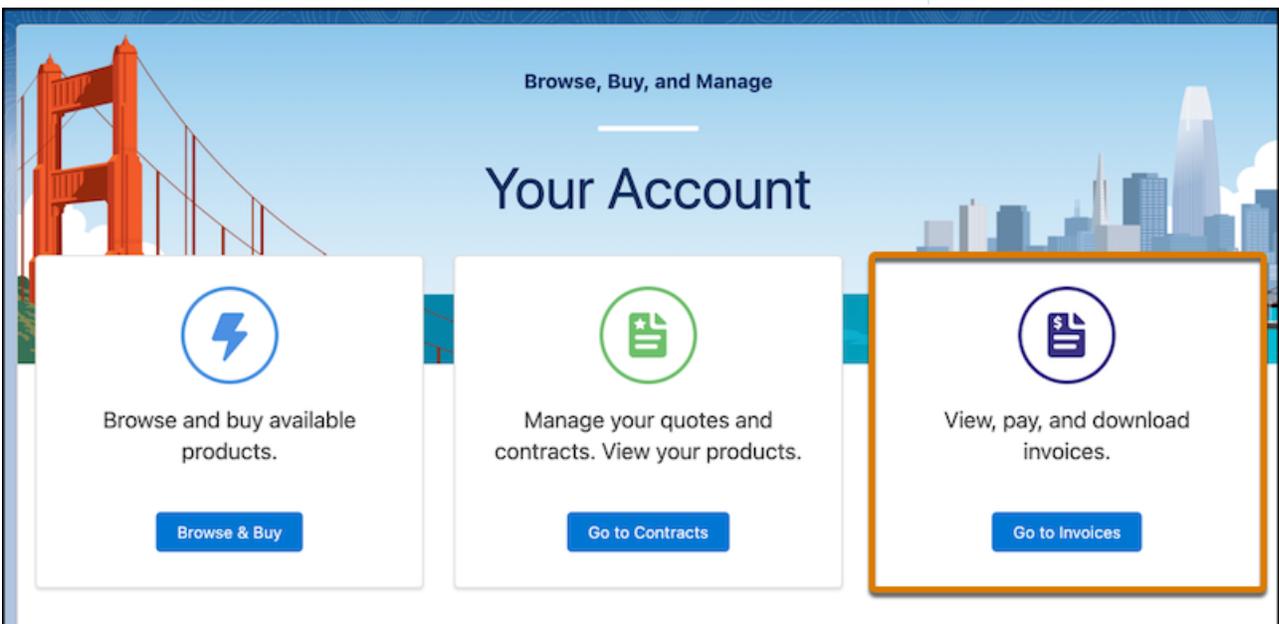
Available in: Salesforce Classic and Lightning Experience

Available in: **Starter**, **Professional**, **Enterprise**, **Performance**, and **Unlimited** Editions

USER PERMISSIONS

To use the Your Account app:

- Manage Billing or the Your Account App Admin User permission set



2. In the invoice list, use the filters to display your invoices.

INVOICE	STATUS	CONTRACT	INVOICE DATE	DUE DATE	INVOICE AMOUNT	BALANCE DUE	
4535.0000000F ZP	Due soon	03010507	8/5/2021	12/10/2022	\$1,382.00	\$1,382.00	Pay Now
4535.0000000F ZK	Due soon	03010507	8/5/2021	10/10/2022	\$900.00	\$900.00	Pay Now
4535.0000000F ZH	Past due	03010506	8/5/2021	8/5/2021	\$498.00	\$498.00	Pay Now
4535.0000000F ZM	Pending	03010506	8/5/2021	2/2/2021	\$4,086.00	\$4,086.00	Pay Now

- To view invoice details, click an invoice number.

PRODUCT	START DATE	END DATE	QUANTITY	TOTAL AMOUNT
Data Storage (100MB)	8/6/2021	8/27/2021	2	\$192.50
Data Storage (100MB)	8/06/2021	8/27/2021	2	\$200.00

 **Note:** Some past due invoices can be paid online. If the Make a Payment button isn't available, contact [Salesforce Billing](#) for help.

Get Support with the Your Account App

Ask product questions, manage billing, get technical support, and send us feedback, all from the Your Account app. Find these contact options on the app's home page.

Determine who to contact based on what you need.

Your Need	How to Get Support
Which products work best for my business?	Email your Account Contact using the email address on the app's home page.
I want to renew my account contract or a product subscription.	Contact Support through our Support form on the app's home page.
I have a billing question.	Contact Support through our Support form on the app's home page.
Something's not working right.	Contact Support through our Support form on the app's home page.
I have a feature request or other product observation to share.	Fill out our feedback form .

Locate contact information on the home page of the Your Account app:

EDITIONS

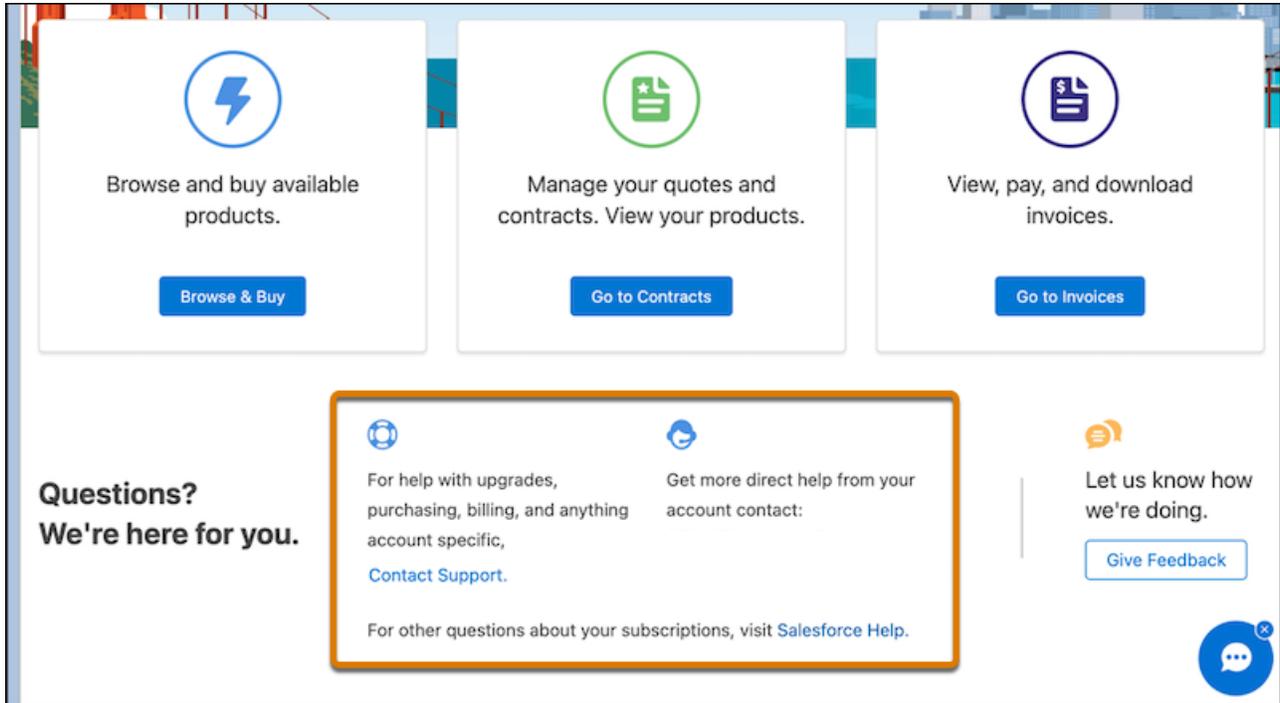
Available in: Salesforce Classic and Lightning Experience

Available in: **Starter**, **Professional**, **Enterprise**, **Performance**, and **Unlimited** Editions

USER PERMISSIONS

To use the Your Account app:

- Manage Billing or the Your Account App Admin User permission set



Turn Off the Your Account App

Use the Your Account app to add products and licenses, manage your contracts and renewals, view invoices, and get account support right in Salesforce. You can turn it off for all your users, but we don't recommend it.

1. From Setup, in the Quick Find box, enter *Manage Subscription*, and then select **Manage Subscription**.
2. To turn off the Your Account app, click **Manage your subscription with Your Account**. Then refresh the page.

EDITIONS

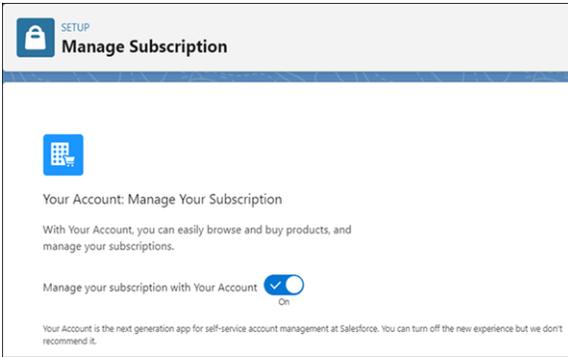
Available in: Salesforce Classic and Lightning Experience

Available in: **Starter**, **Professional**, **Enterprise**, **Performance**, and **Unlimited** Editions

USER PERMISSIONS

To use the Your Account app:

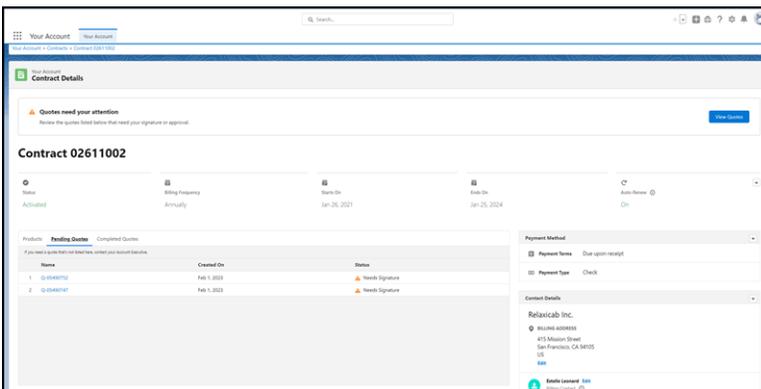
- Manage Billing or the Your Account App Admin User permission set



Manage Your Quotes with the Your Account App

You can manage quotes and complete your purchase using the new Pending Quotes tab on the updated Contract Details page. Review and sign, approve, and place your order using Your Account.

1. Log in to Your Account and select **View Contracts**.
2. Select a contract from the list on the Contracts page.
3. Select the Pending Quotes tab, and then click the quote hyperlink, or select **View Quotes** if the "Quotes need your attention" banner is shown.



4. Review your draft quote.
5. To open a new browser tab for a signature, select **Sign Now**. To receive a link in your email to place your order, select **Sign Later**.

EDITIONS

Available in: **Starter, Professional, Enterprise, Unlimited, and Developer** Editions

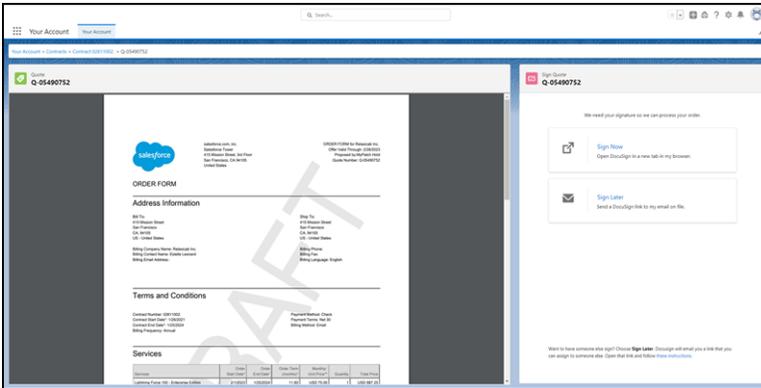
USER PERMISSIONS

To manage, update, and approve quotes:

- Manage Billing permission

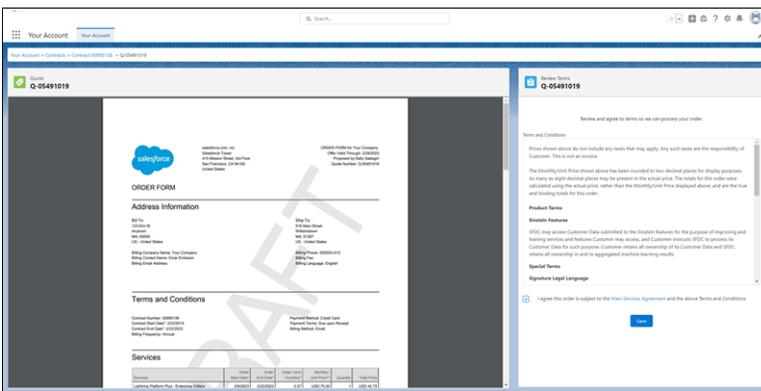
OR

Your Account App Admin permission set



Recent quotes that were signed or approved show Processing as the status in the Pending Quotes tab until the order is completed.

- If you're paying by credit card, use the **Open Quote** button or the hyperlink to open and approve the quote. Select the terms and conditions checkbox and save.



Access Your Completed Quotes with the Your Account App

You can review and download your completed quotes using the new Completed Quotes tab available on the updated Contract Details page in Your Account.

- Log in to Your Account and select **View Contracts**.
- Select a contract from the list on the Contracts page.
- To view the quote before downloading, select the Completed Quotes tab, and then click the quote hyperlink.

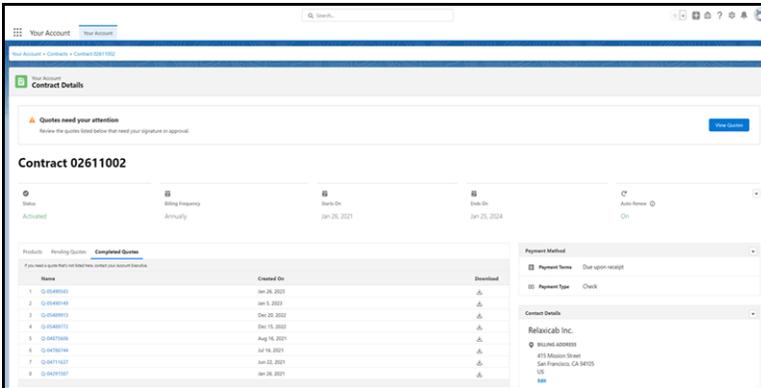
EDITIONS

Available in: **Starter**, **Professional**, **Enterprise**, **Unlimited**, and **Developer Editions**

USER PERMISSIONS

To manage, update, and approve quotes:

- Manage Billing permission
- OR
- Your Account App Admin permission set



- To save a copy locally without reviewing, click the download icon.

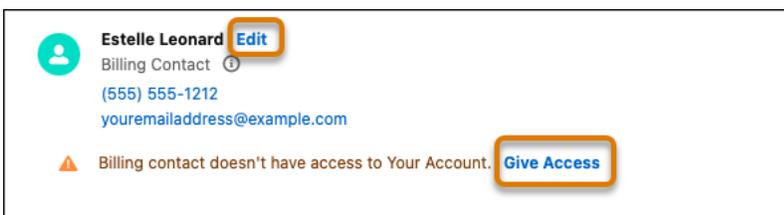
Update Billing Contact Access to the Your Account App

Make sure that the billing contact on each Salesforce contract has access to the Your Account app by granting access from the Contract page. When you give billing contacts access to Your Account, users get the permissions they must have to manage their billing and contracts.

To better control the management of billing activities, Salesforce admins can grant Your Account app access from the Contract page. Admins aren't required to create or update users outside of Your Account, saving additional steps.

- Launch the Your Account app, and then click **View Contracts**.
- Select the contract for which you want to update the billing contact.
- To change the billing contact and grant access to Your Account, click **Edit**.
Doing so assigns the Your Account App Admin permission set, which includes the Manage Billing permission.

If the current billing contact doesn't have access, you see the **Give Access** link. If the user doesn't exist, a user is created using an identity license. The user gets the Your Account App Admin permission set, which includes the Manage Billing permission.



EDITIONS

Available in: **Starter**, **Professional**, **Enterprise**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To use the Your Account app:

- Manage Billing

OR

Your Account App Admin permission set

To give user access to the Your Account app:

- Manage Users

Manage Users

In Salesforce, each user is uniquely identified with a username, password, and profile. Together with other settings, the profile determines which tasks a user can perform, what data the user can see, and what the user can do with the data.

User Management Administration

As a Salesforce administrator, you manage users in your org. Besides creating and assigning users, user management includes working with permissions and licenses, delegating users, and more.

User Management Settings

Manage org-wide user settings to improve user experience and increase org security.

View and Manage Users

In the user list, you can view and manage all users in your org, partner portal, and Salesforce Customer Portal.

Licenses Overview

To enable specific Salesforce functionality for your users, you must choose one user license for each user. To enable more functionality, you can assign permission set licenses and feature licenses to your users or purchase usage-based entitlements for your organization.

Delegate Administrative Duties

Use delegated administration to assign limited admin privileges to users in your org who aren't administrators. For example, let's say you want the Customer Support team manager to manage users in the Support Manager role and all subordinate roles. Create a delegated admin for this purpose so that you can focus on other administration tasks.

Define Delegate Administrators

Enable delegated administrators to manage users in specified roles and all subordinate roles. You can assign specified profiles to those users, and log in as users who have granted login access to administrators. A delegated administration group is a group of users who have the same admin privileges. These groups are not related to public groups used for sharing.

Topics and Tags Settings

Topics on objects allow users to add topics to records so they can organize them by common themes. With Chatter enabled, users can also see related posts and comments. Enabling topics for an object disables public tags on records of that object type. Personal tags aren't affected.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

The available user management options vary according to which Salesforce Edition you have.

User Management Administration

As a Salesforce administrator, you manage users in your org. Besides creating and assigning users, user management includes working with permissions and licenses, delegating users, and more.

! **Important:** Salesforce recommends that you appoint a backup administrator for your org. A backup administrator can keep your org running in case your primary administrator is unavailable.

As an administrator, you perform user management tasks, such as:

- Create and edit users
- Reset passwords
- Create Google Apps accounts
- Grant permissions
- Create and manage other types of users

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

The available user management options vary according to which Salesforce Edition you have.

- Create custom fields
- Set custom links
- Run reports on users
- Delegate user administration tasks to other users

Depending on your Salesforce edition and the additional features that your company purchased, you have specific licenses, such as Marketing or Connect Offline. The licenses let users access features that are not included in their user licenses. Assign one or more licenses to users and set up accounts for users outside your org to access a limited set of fields and objects. You can grant access to the Customer Portal, partner portal, or Self-Service through user licenses. Using Salesforce to Salesforce, create connections to share records with other Salesforce users outside of your org.

 **Note:** Starting with Spring '12, the Self-Service portal isn't available for new Salesforce orgs. Existing orgs continue to have access to the Self-Service portal.

Tips for Managing Users

- Create custom fields for users and set custom links to display on the user detail page. To access these options, go to the object management settings for users.
- Use the sidebar search to search for any user in your org, regardless of the user's status. When using a lookup dialog from fields within records, the search results return only active users. You can also run user reports in the Reports tab.
- To simplify user management in orgs with many of users, delegate aspects of user administration to non-administrator users.

SEE ALSO:

[View and Manage Users](#)

[Licenses Overview](#)

User Management Settings

Manage org-wide user settings to improve user experience and increase org security.

[Enable User Self-Deactivation](#)

Let external Experience Cloud site and Chatter users deactivate their own accounts. The results are identical to an administrator-initiated deactivation.

[Personal User Information Policies and Timelines](#)

To protect your external users' data, Salesforce introduced security settings that let you control personal user information visibility. Use this topic as a starting point to understand all the security improvements and updates, including timelines for enforcement and how to prepare for the changes.

[Manage Personal User Information Visibility for External Users](#)

Protect your external users' data by concealing personal information fields from other external users. To meet your business's security needs, you can modify which user fields are classified as personal information and hidden.

[Personal User Information Considerations](#)

Keep these considerations in mind as you configure personal user information settings for external users by using Enhanced Personal Information Management.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

Custom Profiles available in: **Essentials, Professional, Enterprise, Performance, Unlimited**, and **Developer** Editions

Let Users Scramble Their User Data

When users no longer want their personal data recognized in Salesforce, you can permanently scramble the data with the `System.UserManagement.obfuscateUser` Apex method. However, when you invoke the method for a user, the data becomes anonymous, and you can never recover it. As an extra precaution, you can't use the method until you enable **Scramble Specific Users' Data** for your org.

Enable Contactless Users

Enable the contactless user feature for your org to reduce the overhead of managing customers and partners by creating users without contact information. Without contacts, you don't have to worry about keeping user and contact records in sync. For example, if you maintain a user directory for identity purposes, no contact information is required.

Enable Enhanced Profile List Views

Enhanced lists give you the ability to quickly view, customize, and edit list data to speed up your daily productivity.

Enable Enhanced Permission Set Component Views

When you have large numbers of Apex class assignments for permission sets, enable a paginated result set, standard filtering, and sorting to work more efficiently.

Enable the Enhanced Profile User Interface

The enhanced profile user interface provides a streamlined experience for managing profiles. You can easily navigate, search, and modify settings for a profile. Your Salesforce org can use one profile user interface at a time.

Limit Profile Details to Required Users

Keep Salesforce as secure as possible. Limit users from viewing any profile names other than their own.

Restrict Permissions Cloning in Profiles

Use the Restricted Profile Cloning option to ensure that only permissions accessible to your org are enabled when you clone profiles. If you don't enable this setting, all permissions currently enabled in the source profile are also enabled for the cloned profile, even if your org can't currently access them.

Enable the Email Domain Allowlist

Enable the Email Domain Allowlist Setup page, where you can restrict the email domains allowed in a user's Email field.

Enable Field-Level Security for Permission Sets during Field Creation

Set field-level security for a field on permission sets instead of profiles.

Enable User Access Policies (Beta)

User access policies allow you to automate and migrate your users' assignments to access mechanisms, including managed package licenses, permission sets, and permission set licenses.

Enable User Self-Deactivation

Let external Experience Cloud site and Chatter users deactivate their own accounts. The results are identical to an administrator-initiated deactivation.



Note: Deactivation is not the same as deletion. To learn more about deactivation, refer to Salesforce documentation about deactivating users.

1. From Setup, enter `user` in the Quick Find box, then select **User Management Settings**.
2. Enable **User Self Deactivate**.
3. Use developer or declarative tools to provide a mechanism for users to deactivate their accounts. In Experience Cloud sites built with Aura templates, the [Customizable User Settings component](#) gives users the option to deactivate their account.

EDITIONS

Available in: All Editions

USER PERMISSIONS

To enable external user deactivation option:

- Customize Application

 **Note:** In Experience Cloud sites using LWR or Visualforce templates, create a flow that external users can run to deactivate their own accounts without the help of an admin.

SEE ALSO:

[Delete Users](#)

Personal User Information Policies and Timelines

To protect your external users' data, Salesforce introduced security settings that let you control personal user information visibility. Use this topic as a starting point to understand all the security improvements and updates, including timelines for enforcement and how to prepare for the changes.

The Salesforce security policy encompasses all public sites created in a Salesforce org, including Lightning Platform, Site.com, or Experience Cloud. These settings are included in the policy for personal user information.

Enhanced Personal Information Management Using Field Sets

This setting hides personal information fields in user records from external users. Use a field set to modify which fields are classified as personal information and concealed. If you enabled Enhanced Personal Information Management before Spring '22, you can use Compliance Categorization on user object fields.

When you use the PersonalInfo_EPIM field set to classify fields as personal information, both First Name and Last Name are concealed by default. But you can specify which components of a user's name or address to hide. For example, if you want to make your users' first names visible you can choose to hide Last Name only.

For more information on this setting, see [Manage Personal User Information Visibility for External Users](#).

Enhanced Personal Information Management Using Compliance Categorization

In orgs that enabled this feature before Spring '22, admins manage which personal information fields are visible by using Compliance Categorization on the user object. If your org uses Compliance Categorization, make sure to classify the Name field as personal information.

For more information on this setting, see [Manage Personal User Information Visibility for External Users](#).

Enhanced Personal Information Management and the Show Nicknames Setting

For customers who used the retired Hide Personal Information setting, but haven't enabled the Enhanced Personal Information Management setting, Salesforce still hides some personal information fields in user records from external users. The affected fields are:

- Alias
- EmployeeNumber
- FederationIdentifier
- SenderEmail
- Signature
- Username
- Division
- Title
- Department

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

- Extension

When the Show Nicknames preference is enabled and the following Name fields are classified as PII, the user's nickname is displayed instead of these fields:

- Name
- First Name (component of the Name field)
- Last Name (component of the Name field)

 **Important:** To protect your users' names from being viewed by external users, don't remove Name, First Name, or Last Name from the PersonalInfo_EPIM field set. If your org secures PII using Compliance Categorization, don't remove PII Compliance Categorization from Name, First Name, or Last Name fields.

 **Note:** Enhanced Personal Information Management using Compliance Categorization isn't available in orgs created in Winter '22 or later.

For more information on this setting, see [Show Nicknames Instead of Full Names in an Experience Cloud Site](#).

Timelines for Enforcing Public Site Security Policies

The introduction and enablement timeline of these settings begins in Winter '22. This timeline is subject to change. Check to see what release your org is running on [Salesforce Status](#).

Details of the Winter '22 Updates

The [Enhanced Personal Information Management](#) setting is available in all orgs beginning in Winter '22. For orgs created before Winter '22, this setting is disabled by default and must be enabled by an admin. For orgs created in Winter '22 or later, this setting is enabled by default.

Salesforce orgs that enable the Enhanced Personal Information Management setting in Winter '22 use Compliance Categorization to classify user fields as personal information.

Details of the Spring '22 Updates

In this release, we introduced the Enable Stronger Protection for Your Users' Personal Information release update. Use this release update to test and prepare your org before the Enhanced Personal Information Management setting is automatically enabled in Winter '23.

Salesforce blocks 30 personal information fields using a field set called PersonalInfo_EPIM. You can choose which fields to include in the field set, which provides even more flexibility and scalability.

- Admins who enable Enhanced Personal Information Management in Spring '22 can use field sets to manage which fields are classified as personal information.
- If you enabled the setting before Spring '22, make sure to classify the Name field as personal information. You can use field sets to choose which fields are considered personally identifiable information (PII), or continue to use Compliance Categorization.

Support for the **Show Nicknames** preference is available this release with the Enhanced Personal Information Management setting.

Details of the Summer '22 Updates

In this release, information classified as personal or sensitive is no longer visible to users with View All Users, Modify All Data, and View All Data permissions. To view personally identifiable information, users must have the View Concealed Field Data permission. The View Concealed Field Data permission replaces the View User Records with PII permission.

Details of the Winter '23 Updates

Enforcement of the Enable Stronger Protection for Your Users' Personal Information release update is postponed to the Spring '23 release.

Details of the Spring '23 Updates

The Enable Stronger Protection for Your Users' Personal Information release update is enforced. The Enhanced Personal Information Management setting is enabled in all orgs. The default user fields classified as personal information are hidden from external users.

Some orgs enabled Digital Experiences and Hide Personal Information, but haven't enabled Enhanced Personal Information Management before Spring '23. For these orgs, the fields listed in this article are protected. Name fields aren't concealed unless Show Nicknames is enabled.

If you rely on having certain user fields exposed to external users, you must remove them from the PersonalInfo_EPIM field set or modify these fields' Compliance Categorization to restore visibility. To manage the visibility of user fields, you must use Enhanced Personal Information Management.

The Hide Personal Information setting and the **Hide first and last name fields in the SOAP API for site users, when making API calls from within a site with nicknames** setting are retired in all orgs.

 **Important:** We strongly recommend that you adopt this feature and test its impact as soon as possible ensure no unexpected changes in functionality.

SEE ALSO:

[Create and Edit Field Sets](#)

[Guest User Security Policies and Timelines](#)

Manage Personal User Information Visibility for External Users

Protect your external users' data by concealing personal information fields from other external users. To meet your business's security needs, you can modify which user fields are classified as personal information and hidden.

1. From Setup, in the Quick Find box, enter *User Management Settings*, and then select **User Management Settings**.
2. To view and modify fields that are concealed, click **in this field set**.

Review the user fields that are classified as personal information and concealed from authenticated external users, such as portal and community users. Guest users can't view or update personally identifiable information (PII) fields, including their own.

By default, these fields considered PII in the PersonalInfo_EPIM field set.

PII Fields (Spring '22 and After)	Details
About Me	
Alias	
City	Included in field set only; component of Address
Company Name	
Country	Included in field set only; component of Address
Department	

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, and Developer** Editions

Applies to: [LWR, Aura, and Visualforce sites](#)

USER PERMISSIONS

To enable hiding of personal information:

- Customize Application

To view hidden personal information:

- View Concealed Field Data

PII Fields (Spring '22 and After)	Details
Division	
Email	
Email Sender Address	
Email Sender Name	
Email Signature	
Employee Number	
Extension	
Fax	
First Name	Included in field set only; component of Name
Geocode Accuracy	Included in field set only; component of Address
Last Name	Included in field set only; component of Name
Latitude	Included in field set only; component of Address
Longitude	Included in field set only; component of Address
Manager	
MobilePhone	
Name	
Postal Code	Included in field set only; component of Address
SAML Federation ID	
State	Included in field set only; component of Address
Street	Included in field set only; component of Address
Title	
User Photo badge text overlay	
Username	

When you use a field set to classify fields as personal information, you can specify which components of a user's name or address to hide. For example, if you want to make your users' first names visible you can choose to hide Last Name only.

Before Spring '22, admins managed personal information visibility by adding PII to fields on the user object as the Compliance Categorization value. By default, these fields are considered PII in orgs that enabled Enhanced Personal Information Management before or during Spring '22.

 **Important:** Keep name-related personal information secure by enabling the Show Nicknames preference at the site level and using Compliance Categorization on Name fields. Unless you enable Show Nicknames and use PII as the Compliance Categorization value for Name fields on the user object, the First Name and Last Name fields are visible to external users.

PII Fields (Before Spring '22)	Details
About Me	
Address	Available using Compliance Categorization only
Alias	
Company Name	
Department	
Division	
Email	
Email Sender Address	
Email Sender Name	
Email Signature	
Employee Number	
Extension	
Fax	
Manager	
Mobile	
Name	Included if Show Nicknames is enabled
Phone	
SAML Federation ID	
Title	
User Photo badge text overlay	
Username	

When the setting is enabled, external users who search or view user records don't see other users' personal information fields on Experience Cloud sites. Authenticated external users can still view and update their own personal information fields.

- To customize the user fields that are concealed, add them to the PersonalInfo_EPIM field set.

 **Important:** Don't classify fields that don't contain PII. [System fields](#), formula fields, the Default Currency ISO Code field, and the Information Currency field also aren't supported.

 **Note:** If you enabled the setting before Spring '22, continue to use Compliance Categorization to choose which fields are considered PII.

- In Object Manager, select **User**.
- Click **Field Sets**, and then select **PersonalInfo_EPIM**.
- Drag the field into the PersonalInfo_EPIM field set.

- d. Save your work.
 - 4. Alternatively, to customize the user fields that are concealed, change their Compliance Categorization value.
 - a. In Object Manager, select **User**.
 - b. Click **Fields & Relationships**.
 - c. Click the name of the field whose value you want to hide or make visible.
 - d. Click **Edit**.
 - e. To hide the field from external users, select **PII** as the Compliance Categorization value for the field. Removing this Compliance Categorization value exposes the field, which means that external users can see this field's value.
-  **Important:** Don't classify fields that don't contain PII, such as [system fields](#).
- f. Save your work.

SEE ALSO:

[Data Classification Metadata Fields](#)[Classify Sensitive Data to Support Data Management Policies](#)[Create and Edit Field Sets](#)[Personal User Information Policies and Timelines](#)

Personal User Information Considerations

Keep these considerations in mind as you configure personal user information settings for external users by using Enhanced Personal Information Management.

Apex

This setting isn't enforced in Apex, even with security features such as the `WITH SECURITY_ENFORCED` clause or the `stripInaccessible` method. To hide specific fields on the User object in Apex, use the sample code outlined in [Comply with a User's Personal Information Visibility Settings](#).

Automated Tools and Processes

Some workflows, flows, or automated tools send emails in the context of an external user. If the email template references merge fields from another user record, errors can occur.

Workflows, flows, and automated tools that run in system mode don't enforce the personal information visibility settings.

Integrations

Integrations that rely on authentication of an external user can have errors if they sync user data classified as personal information to or from Salesforce.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

Applies to: [LWR](#), [Aura](#), and [Visualforce sites](#)

Permissions

Information classified as personal or sensitive isn't visible to users with View All Users, Modify All Data, and View All Data permissions. To view personally identifiable information (PII), a user must have the View Concealed Field Data permission.

Profile Pages

Profile pages in Experience Cloud sites can display blank fields for the protected information when viewed by other site users or guest users. Authenticated external users can still see and modify their personal information when viewing their own profile pages, with some exceptions:

- If any address field is considered PII, the whole address field is hidden. Address fields include City, State, Street, Postal Code, Country, GeocodeAccuracy, Latitude, and Longitude.
- When the First Name or Last Name field is considered PII, a nickname is shown when nickname display is enabled. When nickname display isn't enabled, name fields are visible.
- When some but not all address fields are considered PII, guest users have a different experience than community or portal users. If at least one address field is included in the PersonallInfo_EPIM field set, all address fields are blocked for guest users. But in this scenario, community and portal users can see address fields that aren't in the field set, even if other address fields were added.



Example: An admin enables Enhanced Personal Information Management then removes these address fields from the PersonallInfo_EPIM field set: Zip/Postal Code, Country. Next, the admin contacts a guest user and a community user to test the setting that they enabled.

- The guest user navigates to another user's profile page in Salesforce. None of the address fields show address information. The Zip/Postal Code and Country fields, which weren't included in the field set but are elements of the address compound field, are hidden.
- The community user navigates to another user's profile page. Address fields that are included in the PersonallInfo_EPIM field set, such as Street and City, are hidden. But address fields that weren't included, such as the Zip/Postal Code and Country fields, are visible.

To ensure that User PII data is protected, the admin returns to the PersonallInfo_EPIM field set, adding the Zip/Postal Code and Country fields to it.

- The guest user again navigates to another user's profile page. None of the address fields show address information. This information is still hidden.
- The community user navigates to another user's profile page. Address fields such as Country are still not visible, and the Zip/Postal Code and Country fields are no longer visible.

Reports and Dashboards

If a report or dashboard subscription has the running user set as an internal user, external user recipients can see user fields classified as personal information.

Let's say a dashboard subscription has the running user set as an internal user, and the dashboard returns user fields that are classified as personal information. An external user who is subscribed to the dashboard can see these fields, even though they're classified as personal information.

Supported Fields

- You can hide any standard or custom user field except for [system fields](#), formula fields, the Default Currency ISO Code field, and the Information Currency field.
- Don't classify fields that don't contain PII.

- If you classify the Name field as personally identifiable and enable the Show Nicknames preference for your Experience Cloud site, external and guest users see Nickname in Name fields. When you use field sets, you can also choose whether to classify first and last name as PII. If the First Name field isn't PII, but the Last Name field is, the First Name field displays the first name. The Last Name field displays the nickname.
- When using a field set to hide PII fields, you can classify compound fields, such as Name or Address, as personal information by adding them to the field set. You can also configure personal information visibility for the individual component fields that are displayed in the default PersonalInfo_EPIM field set, such as City.
- When using Compliance Categorization to hide PII fields, you can configure personal information visibility for compound fields only that appear in Object Manager, such as Address. You can't classify their individual component fields, such as City or Postal Code, as personal information.

Other Considerations

- If you use a field set to hide PII fields, you can use a change set or an unlocked package to move the field set from one org to another. If you've migrated from using Compliance Categorization to using a field set, add the Name field to the field set to ensure that names are hidden.
- When you use Compliance Categorization to hide PII fields, the Setup Audit Trail includes each instance when you added or removed the **PersonalInfo** value for a field. When you use field sets, the audit trail shows only that the field set was updated.

SEE ALSO:

[Manage Personal User Information Visibility for External Users](#)

Let Users Scramble Their User Data

When users no longer want their personal data recognized in Salesforce, you can permanently scramble the data with the `System.UserManagement.obfuscateUser` Apex method. However, when you invoke the method for a user, the data becomes anonymous, and you can never recover it. As an extra precaution, you can't use the method until you enable **Scramble Specific Users' Data** for your org.

1. From Setup, enter `USER` in the Quick Find box, then select **User Management Settings**.
2. Enable **Scramble Specific Users' Data**.
3. Invoke the `obfuscateUser` method one of several ways. For example, you can use custom Apex triggers, processes, workflows, or the Developer Console.

 **Note:** Invoking `obfuscateUser` method doesn't trigger an email change notification.

This feature is part of our effort to protect users' personal data and privacy. For more information on what you can do to actively protect user data, see [Data Protection and Privacy](#).

For more information about `obfuscateUser`, see the `UserManagement` Class in the *Apex Reference Guide*.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To enable the Scramble Specific Users' Data setting:

- [Customize Application](#)

Enable Contactless Users

Enable the contactless user feature for your org to reduce the overhead of managing customers and partners by creating users without contact information. Without contacts, you don't have to worry about keeping user and contact records in sync. For example, if you maintain a user directory for identity purposes, no contact information is required.

 **Note:** The contactless users feature is available only with the External Identity license, which enables access to the Salesforce Customer Identity product.

1. From Setup, enter `user` in the Quick Find box, then select **User Management Settings**.
2. Select **Contactless Salesforce Customer Identity Users**.

If you later want to upgrade users to a full community license, you must first add contact information to the user record.

SEE ALSO:

[Manage Contactless Users](#)

Enable Enhanced Profile List Views

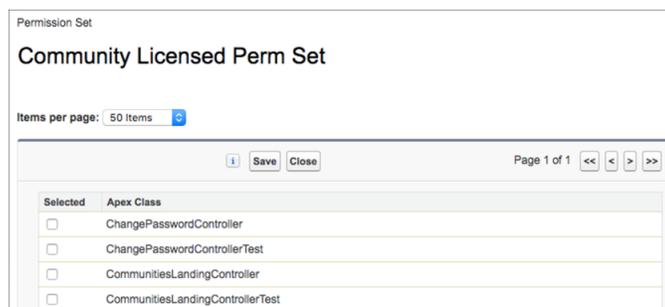
Enhanced lists give you the ability to quickly view, customize, and edit list data to speed up your daily productivity.

1. From Setup, enter `user` in the Quick Find box, then select **User Management Settings**.
2. Enable **Enhanced Profile User Interface**.

Enable Enhanced Permission Set Component Views

When you have large numbers of Apex class assignments for permission sets, enable a paginated result set, standard filtering, and sorting to work more efficiently.

1. From Setup, enter `user` in the Quick Find box, then select **User Management Settings**.
2. Enable **Enhanced Permission Set Component Views**.
Select a permission set and then select **Apex Class Access** and click **Edit**. If you have many classes assigned to the permission set, select the number of items per page to view. Also use arrows to scroll through pages.



EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise, Performance, Professional, Unlimited, and Developer** Editions

USER PERMISSIONS

To enable Contactless User setting:

- Manage Users and Customize Application

USER PERMISSIONS

To enable the enhanced profile list view:

- Customize Application

Enable the Enhanced Profile User Interface

The enhanced profile user interface provides a streamlined experience for managing profiles. You can easily navigate, search, and modify settings for a profile. Your Salesforce org can use one profile user interface at a time.

1. From Setup, in the Quick Find box, enter *user*, and then select **User Management Settings**.
2. Enable **Enhanced Profile User Interface**.
You can't use the enhanced profile user interface for your org if:
 - You use Microsoft® Internet Explorer® 6, which is now obsolete. Support for Internet Explorer ended December 2020. Replace it with Microsoft Edge.
 - You use category groups on guest profiles used for sites.
 - You delegate partner portal administration to portal users.

SEE ALSO:

[Configure Default Settings in Profiles Profiles](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

Custom Profiles available in: **Essentials, Professional, Enterprise, Performance, Unlimited**, and **Developer** Editions

USER PERMISSIONS

To enable the enhanced profile user interface:

- Customize Application

Limit Profile Details to Required Users

Keep Salesforce as secure as possible. Limit users from viewing any profile names other than their own.

If profile filtering is disabled, users can see all profile names, regardless of which permissions they have. If you enable profile filtering, you can restrict who sees profile information to the users who require the access for their job roles. To allow selected users to view all profiles, you can enable the View All Profiles permission for them.

1. From Setup, in the Quick Find box, enter *user*, and then select **User Management Settings**.
2. Enable **Profile Filtering**.

With Profile Filtering enabled, some users can still see profile names in specific scenarios. Profile names are exposed when users with permissions to perform these tasks take these actions:

- View the Setup Audit Trail if they have the View Setup and Configuration permission.
- Create a tab or record type with a wizard step that includes the assignment of tabs and record types to profiles.
- Set up delegated admins where looking up profiles is necessary to identify assignable profiles.
- Administer Salesforce as a delegated external user admin.
- Administer Salesforce as a delegated admin to view and assign profiles of the delegated group.

 **Note:** When you enable Profile Filtering, users can't create or edit login flows. To give users access to login flows, enable the View All Profiles permission.

SEE ALSO:

[User Permissions](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

Custom Profiles available in: **Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To enable profile filtering:

- [Customize Application](#)

Restrict Permissions Cloning in Profiles

Use the Restricted Profile Cloning option to ensure that only permissions accessible to your org are enabled when you clone profiles. If you don't enable this setting, all permissions currently enabled in the source profile are also enabled for the cloned profile, even if your org can't currently access them.

1. From Setup, enter *User* in the Quick Find box, then select **User Management Settings**.
2. Enable **Restricted Profile Cloning**.

When you clone profiles, only permissions currently allowed in your org are enabled for the cloned profiles.

 **Example:** Let's say that you previously enabled Quotes in your org, so the Standard User profile has access to the feature. If you disable Quotes, then object permissions related to the feature, such as Quote, Products and Price Books, are no longer accessible from the Standard User profile. If you clone the Standard User profile and enable Quotes again, both the Standard User profile and the cloned profile have the relevant object permissions enabled.

You might intend to enable Quotes for both the Standard User profile and the cloned profile. But cloned profiles typically have different purposes than the profiles they are cloned from. To ensure that only the intended profiles receive permissions for specific functionality, enable **Restricted Profile Cloning**.

SEE ALSO:

[Create or Clone Profiles](#)

Enable the Email Domain Allowlist

Enable the Email Domain Allowlist Setup page, where you can restrict the email domains allowed in a user's Email field.

1. From Setup, in the Quick Find box, enter *User Management Settings*, and then select **User Management Settings**.
2. Turn on **Email Domain Allowlist**.

When the allowlist is enabled, you can access the Allowed Email Domains Setup page.

SEE ALSO:

[Restrict User Email Domains](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

Custom Profiles available in: **Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To enable restricted profile cloning option:

- [Customize Application](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

USER PERMISSIONS

To enable Allowed Email Domains:

- [Customize Application](#)

Enable Field-Level Security for Permission Sets during Field Creation

Set field-level security for a field on permission sets instead of profiles.

1. From Setup, in the Quick Find box, enter *User Management Settings*, and then select **User Management Settings**.
2. Enable **Field-Level Security for Permission Sets during Field Creation**.

 **Example:** To follow best practices for user access control, you plan to assign permissions through permission sets and permission set groups. For easier permission set management, turn on **Field-Level Security for Permission Sets during Field Creation**. When you create a field, you can then set field-level security on your permission sets as part of the workflow.

Now when you create a field on an object, set field-level security on a field, or change a field's type, you assign field-level security for permission sets instead of profiles.

 **Note:** The View Field Accessibility page doesn't currently support permission sets.

SEE ALSO:

[Create Custom Fields](#)

[Set Field-Level Security for a Field on All Permission Sets](#)

Enable User Access Policies (Beta)

User access policies allow you to automate and migrate your users' assignments to access mechanisms, including managed package licenses, permission sets, and permission set licenses.

 **Note:** This feature is a Beta Service. Customer may opt to try such Beta Service in its sole discretion. Any use of the Beta Service is subject to the applicable Beta Services Terms provided at [Agreements and Terms](#).

1. From Setup, in the Quick Find box, enter *User Management Settings*, and then select **User Management Settings**.
2. Enable **User Access Policies (Beta)**.

If Salesforce enabled user access policies for you before the Summer '23 release, you must enable this feature again on the User Management Settings page.

SEE ALSO:

[User Access Policies \(Beta\)](#)

EDITIONS

Available in: all editions

USER PERMISSIONS

To enable setting field-level security for permission sets instead of profiles during field creation:

- [Customize Application](#)

EDITIONS

Available in: both Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: **Enterprise** and **Unlimited** editions

USER PERMISSIONS

To enable User Access Policies:

- [Manage Users](#)

View and Manage Users

In the user list, you can view and manage all users in your org, partner portal, and Salesforce Customer Portal.

From Setup, enter *Users* in the **Quick Find** box, then select **Users**.

From the user list, you can:

- Create one user or multiple users.
- Reset passwords for selected users.
- Edit a user.
- View a user's detail page by clicking the name, alias, or username.
- View or edit a profile by clicking the profile name.
- If Google Apps™ is enabled in your org, export users to Google and create Google Apps accounts by clicking **Export to Google Apps**.

You can also create and export user reports. For more information, see [Administrative Reports](#).

[Administrators and Separation of Duties](#)

Separating duties limits the power of any one person or entity so that you can help prevent a single point of failure. For example, you can have two or more administrators who have responsibilities for administering different portions of your org. If you have only one administrator, consider assigning a backup person to the role. You can give the backup person the same access that your primary administrator has.

[Guidelines for Adding Users](#)

Understand important options for adding users. Learn what to communicate to users about passwords and logging in.

[Add a Single User](#)

Depending on the size of your organization or your new hire onboarding process, you may choose to add users one at a time. The maximum number of users you can add is determined by your Salesforce edition.

[Add Multiple Users](#)

You can quickly add up to 10 users at a time to your organization. Your Salesforce edition determines the maximum number of users that you can add.

[Edit Users](#)

To change user details—such as a user's profile, role, or contact information—edit the user account.

[Considerations for Editing Users](#)

Be aware of these behaviors when editing users.

[Unlock Users](#)

Users can be locked out of their org when they enter incorrect login credentials too many times. Unlock users to restore their access.

[Delete Users](#)

While you can't completely delete a user, you can deactivate a user's account so they can't log in to Salesforce.

[Freeze or Unfreeze User Accounts](#)

In some cases, you can't immediately deactivate an account, such as when a user is selected in a custom hierarchy field. To prevent users from logging in to your organization while you perform the steps to deactivate them, you can freeze user accounts.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Essentials, Group, Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

Customer Portal and partner portals aren't available in **Database.com**

USER PERMISSIONS

To view user lists:

- View Setup and Configuration

To manage profiles and to log in as a user:

- Manage Users

[Manage Contactless Users](#)

By default, when Salesforce creates a user record for a customer or partner, it adds the user's contact information. But if your implementation doesn't require contact information for customers or partners, consider going contactless to reduce the overhead of managing these types of users. Without contacts, you don't have to worry about keeping user and contact records in sync. For example, if you maintain a user directory for identity purposes, no contact information is required.

[Restrict User Email Domains](#)

You can define an allowlist to restrict the email domains allowed in a user's `Email` field.

[User Fields](#)

The fields that comprise the Personal Information and other personal settings pages describe a user.

Administrators and Separation of Duties

Separating duties limits the power of any one person or entity so that you can help prevent a single point of failure. For example, you can have two or more administrators who have responsibilities for administering different portions of your org. If you have only one administrator, consider assigning a backup person to the role. You can give the backup person the same access that your primary administrator has.

While the practice of having one person perform all administrative duties can make sense, it can lead to troubles. For example, what if:

- Your administrator falls ill, and a mission-critical change must be made to your org.
- Your administrator left your company on unhappy terms but is the only person who has the administrator profile credentials.

Prevent possible problems by ensuring that more than one person can perform key administrative tasks. Consider implementing a process to ensure business continuity if your sole administrator is unavailable. You can also delegate administration tasks by assigning a delegated administrator.

SEE ALSO:

[Add a Single User](#)

[Delegate Administrative Duties](#)

Guidelines for Adding Users

Understand important options for adding users. Learn what to communicate to users about passwords and logging in.

- Your username must be unique across all Salesforce orgs, including trial and Sandbox orgs. The username must be in the format of an email address, for example, jane@salesforce.com. The email used in your username need not function or match the email address used for the account. You can have the same email address associated with your account across multiple orgs. For example, create unique usernames like jane@company.sandbox and jane@trialorg.company.com, for different accounts that are associated with the same email address. Keep in mind that Salesforce Customer Support can't change usernames or deactivate users from an org. If you get a Duplicate Username error, check if the username is already in use in your production, trial, or Sandbox orgs. Deactivate or change the username for the user record, then create your account with your desired username in your production org. If you're unable to change or

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

The availability of each permission set license depends on the edition requirements for permission sets and the related feature.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Essentials, Group, Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

deactivate a username, contact your Salesforce admin for help. If you're unable to locate the org where the username is already in use, try a different username to create your account.

- If your name includes non-English characters and you use Outlook, add the specified language to the mail format settings within Outlook.
- The account verification link emailed to new users expires after 7 days, and users must change their password the first time they log in. Users who click the account verification link but don't set a password need an admin to reset their password before they can log in.
- Not all options are available for all license types. For example, the Marketing User and Allow Forecasting options aren't available for Lightning Platform user licenses because the Forecasts and Campaigns tabs aren't available to Lightning Platform license users. Lightning Platform user licenses are not available for Professional, Group, or Contact Manager Editions.
- In Performance, Unlimited, Enterprise, and Developer Edition orgs, you can select **Send Apex Warning Emails**. This option sends an email to the user when an application that invokes Apex uses more than half of the resources specified by the governor limits. You can use this feature during Apex code development to test the amount of resources used at runtime.
- You can move users between profiles based on user licenses that have the same record sharing models. For example, you can move a Lightning Platform-based profile user to a Salesforce-based profile, or vice versa. The user sometimes loses permission access depending on what the user licenses permit. If you move a user with permission set assignments, the user is removed from the permission set. If you try to add the user back to the permission set, you receive a licensing error unless the new license allows the permissions.

SEE ALSO:

[Add a Single User](#)

[Administrators and Separation of Duties](#)

Add a Single User

Depending on the size of your organization or your new hire onboarding process, you may choose to add users one at a time. The maximum number of users you can add is determined by your Salesforce edition.

1. Read the guidelines for adding users.
2. From Setup, in the Quick Find box, enter `Users`, and then select **Users**.
3. Click **New User**.
4. Enter the user's name and email address and a unique username in the form of a email address. By default, the username is the same as the email address.

 **Important:** Your username must be unique across all Salesforce orgs, including trial and Sandbox orgs. The username must be in the format of an email address, for example, jane@salesforce.com. The email used in your username need not function or match the email address used for the account. You can have the same email address associated with your account across multiple orgs. For example, create unique usernames like jane@company.sandbox and jane@trialorg.company.com, for different accounts that are associated with the same email address. Keep in mind that Salesforce Customer Support can't change usernames or deactivate users from an org. If you get a Duplicate Username error, check if the username is already in use in your production, trial, or Sandbox orgs. Deactivate or change the username for the user record, then create your account with your desired username in your production org. If you're unable to change or deactivate

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Essentials, Group, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To create users:

- Manage Internal Users

a username, contact your Salesforce admin for help. If you're unable to locate the org where the username is already in use, try a different username to create your account.

5. In Professional, Enterprise, Unlimited, Performance, and Developer Editions, select a `Role`.
6. Select a `User License`. The user license determines which profiles are available for the user.
7. Select a profile, which specifies the user's minimum permissions and access settings.
8. If your organization has Approvals enabled, you can set the user's approver settings, such as delegated approver, manager, and preference for receiving approval request emails.
9. Check `Generate new password and notify user immediately` to have the user's login name and a temporary password emailed to the new user.

For new Chatter Only users, an administrator must expose the tabs for accounts, contacts, dashboards, and reports. By default, these tabs are hidden for Chatter Only users. And, the admin must turn on Salesforce CRM Content, Ideas, and Answers if they want their Chatter Only users to have access to them. Professional Edition organizations must have Profiles enabled to perform these tasks. For more information, contact Salesforce Customer Support.

SEE ALSO:

- [Guidelines for Adding Users](#)
- [Add Multiple Users](#)
- [Edit Users](#)
- [User Fields](#)
- [Licenses Overview](#)

Add Multiple Users

You can quickly add up to 10 users at a time to your organization. Your Salesforce edition determines the maximum number of users that you can add.

1. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.
2. Click **Add Multiple Users**.
3. If multiple user license types are available in your organization, select the user license to associate with the users you plan to create. The user license determines the available profiles.
4. Specify the information for each user.
5. To email a login name and temporary password to each new user, select **Generate passwords and notify user via email**.
6. Click **Save**.
7. To specify more details for the users that you've created with this method, edit individual users as needed.

SEE ALSO:

- [Add a Single User](#)
- [Edit Users](#)
- [User Fields](#)
- [Licenses Overview](#)

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To create users:

- [Manage Internal Users](#)

Edit Users

To change user details—such as a user’s profile, role, or contact information—edit the user account.

1. From Setup, enter *Users* in the **Quick Find** box, then select **Users**.
2. Click **Edit** next to a user’s name.
3. Change the settings as needed.
4. Click **Save**.

SEE ALSO:

- [Delete Users](#)
- [Considerations for Editing Users](#)
- [User Fields](#)
- [Unlock Users](#)
- [Licenses Overview](#)

Considerations for Editing Users

Be aware of these behaviors when editing users.

Username

Username must be unique across all Salesforce orgs, including trial and Sandbox orgs. The username must be in the format of an email address, for example, jane@salesforce.com. The email used in your username need not function or match the email address used for the account. You can have the same email address associated with your account across multiple orgs. For example, create unique usernames like jane@company.sandbox and jane@trialorg.company.com, for different accounts that are associated with the same email address. Keep in mind that Salesforce Customer Support can’t change usernames or deactivate users from an org. If you get a Duplicate Username error, check if the username is already in use in your production, trial, or Sandbox orgs. Deactivate or change the username for the user record, then create your account with your desired username in your production org. If you’re unable to change or deactivate a username, contact your Salesforce admin for help. If you’re unable to locate the org where the username is already in use, try a different username to create your account.

If you change a username, a confirmation email with a login link is sent to the email address associated with that user account. If an organization has multiple login servers, sometimes users can’t log in immediately after you change their usernames. The change can take up to 24 hours to replicate to all servers.

Changing email addresses

If you change a user’s email address and the Generate new password and notify user immediately setting is disabled, Salesforce sends a confirmation message to the updated email address. Before the new email address is active, the user must click the link provided in the message.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Essentials, Group, Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To edit users:

- Manage Internal Users

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Essentials, Group, Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

If a user changes their own email address, Salesforce sends a confirmation message to the user's new email address and a verification code to the old address. When the user receives the confirmation email, they must enter the verification code to finish updating their email address.

If you change a user's email address and the Generate new password and notify user immediately setting is enabled, Salesforce sends a password reset link to the new email address. Before the new email address is active, the user must create a new password.

The Generate new password and notify user immediately setting is available by default to orgs created after Summer '21. For orgs created before Summer '21, contact Salesforce customer support to enable it.

Personal information

Users can change their personal information after they log in.

User Sharing

If the organization-wide default for the user object is Private, users must have Read or Write access to the target user to access that user's information.

Domain Names

You can restrict the domain names of users' email addresses to a list of specific domains. Any attempt to set an email address with another domain results in an error message. To enable this functionality for your organization, contact Salesforce.

SEE ALSO:

[Edit Users](#)

Unlock Users

Users can be locked out of their org when they enter incorrect login credentials too many times. Unlock users to restore their access.

To set the maximum number of failed login attempts that are allowed for all user accounts in your org in Password Policies, see [Set Password Policies](#).

1. From Setup, enter `users` in the Quick Find box, then select **Users**.
2. Select the locked user.
You can view the number of failed login attempts for the user's account in the Failed Login Attempts field. When the maximum number of failed login attempts is reached, the counter resets and the user's account is locked. If there's a successful login before the maximum number of failed login attempts is reached, the counter resets and the user's account remains unlocked.
3. Click **Unlock**.
This button appears only when a user is locked out.

SEE ALSO:

[Edit Users](#)

[Set Password Policies](#)

Delete Users

While you can't completely delete a user, you can deactivate a user's account so they can't log in to Salesforce.

Salesforce lets you deactivate users, but not delete them outright. A user can own accounts, leads, and groups, and can be on multiple teams. Removing a user from Salesforce affects many processes in the org. After departure from the org, you obviously don't want the user to retain access to their account. However, merely deleting a user can result in orphaned records and the loss of critical business information.

For these reasons, deactivating rather than deleting the user is the appropriate action to take. Deactivation removes the user's login access, but it preserves all historical activity and records, making it easy to transfer ownership to other users. For situations where changing ownership to other users must be done before deactivation, freezing the user prevents login to the org and access to the user's accounts.

[Deactivate Users](#)

To deactivate a user's account so they can no longer log into Salesforce, complete these steps.

[Considerations for Deactivating Users](#)

Note these considerations when deactivating users.

[Mass Transfer Records](#)

Use the Mass Transfer tool to transfer multiple accounts, leads, service contracts, and custom objects from one user to another.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Essentials, Group, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To view the number of failed login attempts for a user account:

- Manage Users

To unlock users:

- Manage Internal Users

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Essentials, Contact Manager, Group, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To deactivate users:

- Manage Internal Users

Deactivate Users

To deactivate a user's account so they can no longer log into Salesforce, complete these steps.

You can deactivate users, but you can't delete them outright. Deleting a user can result in orphaned records and the loss of critical business information. Deactivating a user prevents access but preserves all historical activity and records.

1. From Setup, in the Quick Find box, enter *users*, then select **Users**.
2. Click **Edit** next to a user's name.
3. Deselect the **Active** checkbox, and then click **Save**.

Watch a Demo: [▶ Removing Users' Access to Salesforce \(Salesforce Classic—English only\)](#)

Keep in mind that after deactivation:

- The user remains in the list of users, but is shown as not active.
- The user still appears as a member of public groups they've been a part of and any default accounts and sales teams.
- Deactivating the user doesn't affect the records they owned until ownership is transferred to others.
- All the user's overrides remain, but they're frozen.
- In Chatter, the user's profile remains, but it shows they're inactive. However, the user remains the owner of any Chatter group they owned until an admin reassigns ownership.

You're prevented from deactivating a user if the user is the:

- default owner of leads
- default or automated case owner
- default lead creator or owner
- default workflow user
- recipient of a workflow email alert
- a user selected in a custom hierarchy field
- a customer portal administrator.

In these cases you can prevent the user from accessing their accounts by freezing them. Freezing a user is done from the user's User Record. Later, after updating ownership and other processes, you can deactivate the user's account.

Finally, if the deactivated user was an approver, you must remove the user from all approval processes, or reassign their approval responsibilities to other users.

SEE ALSO:

[Considerations for Deactivating Users](#)

[Freeze or Unfreeze User Accounts](#)

[Mass Transfer Records](#)

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Essentials, Contact Manager, Group, Professional, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

USER PERMISSIONS

To deactivate users:

- [Manage Internal Users](#)

Considerations for Deactivating Users

Note these considerations when deactivating users.

Situations preventing deactivation

Some situations can prevent you from deactivating a user. In these cases, you must freeze the user's account first to prevent logins while you reassign ownership, memberships, and so on, as needed. Then you can deactivate later.

User licenses and billing

A deactivated user doesn't count against your organization's available user licenses. However, deactivating a user doesn't reduce the number of licenses for which your organization is billed. To change your billing, you must change your organization's license count.

Users in custom hierarchy fields

You can't deactivate a user that's selected in a custom hierarchy field even if you delete the field. To deactivate a user in a custom hierarchy field, delete and permanently erase the field first.

Process Builder

Processes can't update records that are owned by inactive users. When you deactivate a user, also transfer that user's records to an active user to avoid failed processes.

Workflow email alert recipients

You can't deactivate a user that's assigned as the sole recipient of a workflow email alert.

Customer Portal Administrator users

You can't deactivate a user that's selected as a Customer Portal Administrator.

Record access

Deactivated users lose access to any records that were manually shared directly with them, or implicitly shared with them as team members. Users higher in the role hierarchy relative to the deactivated users also lose access to those records. However, you can still transfer their data to other users and view their names on the Users page.

 **Note:** If your organization has asynchronous deletion of obsolete shares enabled, removal of manual and team shares is run during off-peak hours between 6 PM and 4 AM based on your organization's default time zone. For account records, manual and team shares are deleted right after user deactivation.

Deactivated users lose access to shared records immediately. Users higher in the role hierarchy continue to have access until that access is deleted asynchronously. If that visibility is a concern, remove the record access that's granted to the deactivated users before deactivation.

Chatter

If you deactivate users in an organization where Chatter is enabled, they're removed from the Following and Followers lists. If you reactivate the users, the subscription information in the Following and Followers lists is restored.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Essentials, Group, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

If you deactivate multiple users, subscription information isn't restored for users that follow each other. For example, user A follows user B and user B follows user A. If you deactivate users A and B, their subscriptions to each other are deleted from Following and Followers lists. If user A and user B are then reactivated, their subscriptions to each other aren't restored.

Salesforce Files

Files owned by a deactivated user aren't deleted. The deactivated user is the file owner until an admin reassigns the files to an active user. Files shared in a content library can be edited by other library members with author or delete permissions. Sharing rules remain active until an admin modifies them.

Created By fields

Inactive users can be listed in `Created By` fields even when they're no longer active in an organization. Some system operations create records and toggle preferences, acting as an arbitrary administrator user to complete the task. This user can be active or inactive.

Accounts and opportunities owned by deactivated users

You can create and edit accounts, opportunities, and custom object records that are owned by inactive users. For example, you can edit the `Account Name` field on an opportunity record that's owned by an inactive user. This feature requires administrator setup.

Enterprise Territory Management

Deactivated users are no longer assigned to territories and are removed from the territories they were assigned to.

Account and Opportunity Teams

Deactivated users are removed from the default opportunity and account teams of other users. The deactivated users' default opportunity and account teams aren't removed.

When a user on an account team or opportunity team who has Read/Write access (Account Access, Contact Access, Opportunity Access, and Case Access) is deactivated and then reactivated, access defaults to Read Only.

Opportunity teams

If you deactivate users in an org where opportunity splits are enabled, they aren't removed from any opportunity teams where they're assigned a split percentage. To remove a user from an opportunity team, first reassign the split percentage.

Delegated external user administrators

When a delegated external user admin deactivates a portal user, the admin can't remove the portal user from teams that user is a member of.

CRM Analytics

When you deactivate a user who scheduled a dataflow, the dataflow schedule is deleted and the dataflow is unscheduled.

SEE ALSO:

[Delete Users](#)

[Deactivate Users](#)

[Considerations for Deactivating Users](#)

Mass Transfer Records

Use the Mass Transfer tool to transfer multiple accounts, leads, service contracts, and custom objects from one user to another.

To transfer any records that you don't own, you need the required user permissions and read sharing access on the records.

1. From Setup, in the Quick Find box, enter *Mass Transfer Records*, and then select **Mass Transfer Records**.
2. Click the link for the type of record to transfer.
3. Optionally, fill in the name of the existing record owner in the `Transfer from` field. For leads, you can transfer from users or queues.
4. In the `Transfer to` field, fill in the name of new record owner. For leads, you can transfer to users or queues.
5. If your organization uses divisions, select the **Change division...** checkbox to set the division of all transferred records to the new owner's default division.
6. When transferring accounts, you can:
 - Select **Transfer open opportunities not owned by the existing account owner** to transfer open opportunities owned by other users that are associated with the account.
 - Select **Transfer closed opportunities** to transfer closed opportunities associated with the account. This option applies only to closed opportunities owned by the account owner. Closed opportunities owned by other users aren't changed.
 - Select **Transfer open cases owned by the existing account owner** to transfer open cases that are owned by the existing account owner and associated with the account.
 - Select **Transfer closed cases** to transfer closed cases that are owned by the existing account owner and associated with the account.
 - Select **Keep Account Team** to maintain the existing account team associated with the account. If you want to remove the existing account team associated with the account, deselect this checkbox.
 - Select **Keep Opportunity Team on all opportunities** to maintain the existing team on opportunities associated with this account. Any opportunity splits are preserved, and split percentages are assigned to the previous owner transfer to the new one. If this box is unchecked, all opportunity team members and splits are deleted when the opportunity is transferred.

 **Note:** If you transfer closed opportunities, the opportunity team is maintained, regardless of this setting.
7. Enter search criteria that the records you're transferring must match. For example, search accounts in California by specifying *Billing State/Province equals CA*.
8. Click **Find**.

 **Note:** The 'Mass Transfer Records' tool allows up to 250 records at a time. To perform transfers over 250 records, use the Data Loader or another tool.
9. Select the checkbox next to the records that you want to transfer. To select all currently displayed items, check the box in the column header.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Group, Professional, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

Service Contracts available in: **Professional, Enterprise, Performance, Unlimited**, and **Developer** Editions with the Service Cloud

Accounts and Leads not available in: **Database.com**

USER PERMISSIONS

To mass transfer accounts and service contracts:

- Transfer Record
- AND
- Transfer Leads

To mass transfer custom objects:

- Transfer Record

To mass transfer leads:

- Transfer Leads OR Transfer Record

If duplicate records are found, you must select only one of the records to transfer. Transferring duplicate records results in an error.

Duplicate records can appear if you filter leads based on Campaign Member Status and a matching lead has the same campaign member status on multiple campaigns. For example, if you specify *Campaign Member Status equals Sent*, and a matching lead named John Smith has the status Sent on two campaigns, his record displays twice.

10. Click **Transfer**.

When you change record ownership, some associated items that are owned by the current record owner also transfer to the new owner.

Record	Associated items that are also transferred
Accounts	Contacts (on business accounts only), attachments, notes, open activities, open opportunities owned by the current account owner, and optionally, closed opportunities and open opportunities owned by other users.
Leads	Open activities. When transferring leads to a queue, open activities aren't transferred.

When transferring accounts and their related data in Professional, Enterprise, Unlimited, Performance, and Developer Editions, all previous access granted by manual sharing, Apex managed sharing, or sharing rules is removed. New sharing rules are then applied to the data based on the new owner. To grant access to certain users, the new owner must manually share the transferred accounts and opportunities as necessary.

SEE ALSO:

[Transfer Records](#)

Freeze or Unfreeze User Accounts

In some cases, you can't immediately deactivate an account, such as when a user is selected in a custom hierarchy field. To prevent users from logging in to your organization while you perform the steps to deactivate them, you can freeze user accounts.

Let's say a user just left your company. You want to deactivate the account, but the user is selected in a custom hierarchy field. Because you can't immediately deactivate the account, you can freeze it in the meantime.

1. From Setup, enter *Users* in the **Quick Find** box, then select **Users**.
2. Click the username of the account you want to freeze.
3. Click **Freeze** to block access to the account or **Unfreeze** to allow access to the account again.

Freezing user accounts doesn't make their user licenses available for use in your organization. To make their user licenses available, deactivate the accounts.

SEE ALSO:

[Delete Users](#)

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Essentials, Contact Manager, Essentials, Group, Professional, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

USER PERMISSIONS

To freeze or unfreeze user accounts:

- **Manage Users**

Manage Contactless Users

By default, when Salesforce creates a user record for a customer or partner, it adds the user's contact information. But if your implementation doesn't require contact information for customers or partners, consider going contactless to reduce the overhead of managing these types of users. Without contacts, you don't have to worry about keeping user and contact records in sync. For example, if you maintain a user directory for identity purposes, no contact information is required.

You can use contactless users when customers and partners self-register to avoid creating contacts until after the users are qualified. If you want to expand your customer base without depleting your community licenses, start them off as contactless users. Then upgrade them to a full community license when they can benefit from the added features.



Note: The contactless users feature is available only with the External Identity license, which enables access to the Salesforce Customer Identity product.

When using contactless users, consider the following.

- You can't use the Login As feature because it requires contacts.
- Delegated admins can't manage contactless users.
- System for Cross-Domain Identity Management (SCIM) isn't supported when creating contactless users.
- Contactless users have the same access to objects as users with contact information.

[Create Contactless Users](#)

Create users without contact information to reduce the overhead of managing customers and partners. You can add contacts later if you decide that you want them, like when you upgrade to a more full-featured community license. You can add contactless users to new or existing Experience Cloud sites.

[Upgrade a Contactless User to a Community License](#)

Upgrade contactless users with an External Identity license to a community license to give them more access to your Experience Cloud sites. To upgrade a contactless user, you must first assign the user a contact.

[Downgrade Experience Cloud Site Users with Community Licenses to Contactless Users](#)

You can convert Experience Cloud site users with community licenses to contactless users. By converting site users, you can expand your site without adding to the cost. For example, you can downgrade inactive or unqualified users and then upgrade them to full-featured site users later on. You can downgrade users from Setup and through the API.

Create Contactless Users

Create users without contact information to reduce the overhead of managing customers and partners. You can add contacts later if you decide that you want them, like when you upgrade to a more full-featured community license. You can add contactless users to new or existing Experience Cloud sites.

Check that the Contactless External Identity Users feature is enabled for your Salesforce org. For instructions, see [Enable Contactless External Identity Users](#).

 **Note:** The contactless users feature is available only with the External Identity license, which enables access to the Salesforce Customer Identity product.

1. Create a contactless user by creating a user record with Apex, SOAP API, Bulk API, or Bulk API 2.0.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To create contactless users:

- Manage User OR Manage External User OR Edit Self-Service User

```

User u = new User();
    u.FirstName = 'Jane';
    u.LastName = 'Doe';
    u.Email = 'janedoe@test.com';
    u.Alias = 'jane';
    u.Username = 'janedoe@test.com';
    u.CommunityNickname = 'Jane';
    u.LocaleSidKey = 'en_US';
    u.TimeZoneSidKey = 'GMT';
    u.ProfileID = '00exx000000jvN4'; // Profile that's associated with the EI license
    u.LanguageLocaleKey = 'en_US';
    u.EmailEncodingKey = 'UTF-8';
    insert u;
  
```

2. (Optional) Set up self-registration to register customers and partners as contactless users.
 - a. Create a custom self-registration page in Visualforce.
 - b. From Setup, in the Quick Find box, enter *All Sites* and select **All Sites**.
 - c. Next to your site name, click **Workspaces**.
 - d. From Experience Workspaces, select **Administration**, and then select **Login & Registration**.
 - e. Select **Allow customers and partners to self-register**.
 - f. Choose a self-registration page type, and generate a self-registration handler.
 - g. Edit the self-registration handler to create the contactless user programmatically.

Upgrade a Contactless User to a Community License

Upgrade contactless users with an External Identity license to a community license to give them more access to your Experience Cloud sites. To upgrade a contactless user, you must first assign the user a contact.

 **Note:** The contactless users feature is available only with the External Identity license, which enables access to the Salesforce Customer Identity product.

1. To add contact information to a contactless user, update the user's record with Apex, SOAP API, Bulk API, or Bulk API 2.0.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To add a contact to a contactless user:

- Manage User OR Manage External User OR Edit Self-Service User

```
Account a = [SELECT Id FROM Account WHERE Id = '001xx000003DIyf'];
Contact c = new Contact();
c.FirstName = 'Sarah';
c.LastName = 'John';
c.AccountId = a.id;
insert c;
User u = [SELECT Id FROM User WHERE Id = '005xx000001TL1f'];
u.ContactId=c.id;
update u;
```

2. To upgrade to a community license, from Setup, enter *users* in the Quick Find box, then select **Users**.
3. Next to the user you want to upgrade, click **Edit**.
4. Select a community license and profile for the user.
5. Optionally, specify a new profile and role.
6. Save your changes.

Downgrade Experience Cloud Site Users with Community Licenses to Contactless Users

You can convert Experience Cloud site users with community licenses to contactless users. By converting site users, you can expand your site without adding to the cost. For example, you can downgrade inactive or unqualified users and then upgrade them to full-featured site users later on. You can downgrade users from Setup and through the API.

 **Note:** The contactless users feature is available only with the External Identity license, which enables access to the Salesforce Customer Identity product.

Downgrading a site user to a contactless user is a two-step process. You disable the site user and then reactivate the user as a contactless user. When you disable users, Salesforce deactivates them and invalidates their usernames by renaming them. You restore the usernames

when you reactivate the users. Reactivated users receive a Welcome New Member email from Salesforce. You can prevent Salesforce from sending welcome emails from Experience Workspaces.

1. On the user's contact detail page, save the contact's username.
2. From the action dropdown menu, select **Disable User**.
3. (Optional) Disable welcome emails.
 - a. From Experience Workspaces, select **Administration**, and then select **Emails**.
 - b. Under Email Templates, deselect **Send welcome email**.
4. From Setup, in the Quick Find box, enter *Users*, then select **Users**.
5. Next to the user you're downgrading, click **Edit**.
6. For user license, select **External Identity**, and then select a customer or partner profile.
7. Select **Active**.
8. Restore the username name by replacing the username with the one you saved.
9. Save your changes.

You can also downgrade users in bulk from the API. If you're downgrading in bulk, assign the users to a profile. In this example, we're downgrading a single user.

```
//Disable user
String uName;
User u = [SELECT Id, UserName FROM User WHERE Id = '005xx009871TQXL'];
u.IsPortalEnabled=false;
uName = u.UserName;
Update u;

//Activate as a contactless user
User u1 = [SELECT Id, UserName, IsActive FROM User WHERE Id = '005xx009871TQXL'];
u1.UserName = 'sarah@mycompany.com'; // Or uName from above
u1.IsActive = true;
Update u1;
```

Restrict User Email Domains

You can define an allowlist to restrict the email domains allowed in a user's `Email` field.

1. From Setup, in the Quick Find box, enter *Allowed Email Domains*, and then select **Allowed Email Domains**.

 **Note:** If you don't see this page, enable the allowlist. For more information, see [Enable the Email Domain Allowlist](#).

2. Click **New Allowed Email Domain**.

3. Enter a `Domain`.

You can enter a top-level domain, such as *sampledoc.org*, or a subdomain, such as *emea.sampledoc.org*.

4. Click **Save**.

You can repeat the steps to add more email domains to the allowlist.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

USER PERMISSIONS

To restrict user email domains:

- [Manage Users](#)

After you've added one or more email domains, the `Email` field for each new user must match an allowed domain.

The `Email` field for existing users doesn't have to comply with the allowlist. However, if you edit an existing user, update the `Email` field to match an allowed email domain.

 **Note:** The email domain allowlist doesn't apply to users external to your org, such as portal, Experience Cloud site, or Chatter External users.

SEE ALSO:

[Enable the Email Domain Allowlist](#)

[Add a Single User](#)

[Add Multiple Users](#)

[Edit Users](#)

User Fields

The fields that comprise the Personal Information and other personal settings pages describe a user.

The visibility of fields depends on page layouts, user permissions, your org's permissions, and your Salesforce edition.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Field	Description
Accessibility Mode	When selected, enables a user interface mode designed for visually impaired users.
Active	Administrative checkbox that enables or disables user login to the service.
Address	Street address for user. Up to 255 characters are allowed in this field.
Alias	Short name to identify the user on list pages, reports, and other pages where the entire name doesn't fit. Up to 8 characters are allowed in this field.
Allow Forecasting	Indicates whether the user can use Collaborative Forecasts.
Api Token	Indicates whether an API token has been reset. If issues occur, Salesforce uses this field to help you troubleshoot issues related to API tokens.
App Registration: One-Time Password Authenticator	When connected, the user can verify their identity with a code from a third-party authenticator app, such as Google Authenticator, Microsoft Authenticator, or Authy. For example, the user enters a code from the app when logging in from an IP address outside the company's trusted IP range. This type of

Field	Description
	<p>verification code is sometimes called a time-based one-time password, or TOTP.</p> <p>Users with Multi-Factor Authentication for User Interface Logins permission must provide two authentication factors when logging in to Salesforce through the user interface: their username and password, followed by a separate verification method. A current verification code generated by an authenticator app counts as a verification method.</p> <p>If the user has Multi-Factor Authentication for API Logins permission and connects an authenticator app, the user enters the current code from the app to access the service. The user doesn't enter the standard security token.</p>
App Registration: Salesforce Authenticator	<p>When connected, the user can verify their identity by responding to a push notification with the Salesforce Authenticator mobile app, version 2 or later. For example, the user approves a notification when logging in from an IP address outside the company's trusted IP network. If the user sets a trusted location in the app and is allowed to use location-based automated verifications, Salesforce Authenticator can automatically verify the user's identity from that trusted location. Users can connect both Salesforce Authenticator and another authenticator app to the same Salesforce account.</p> <p>When connected, the user can also verify identity with a code from Salesforce Authenticator. For example, the user enters a code from the app when logging in from an IP address outside the company's trusted IP network. This type of verification code is sometimes called a time-based one-time password, or TOTP.</p> <p>Users with Multi-Factor Authentication for User Interface Logins permission must provide two authentication factors when logging in to Salesforce through the user interface: their username and password, followed by a separate verification method. A manual or automated response to a notification from Salesforce Authenticator counts as a verification method.</p> <p>If the user has Multi-Factor Authentication for API Logins permission and connects Salesforce Authenticator, the user enters the current code from the app to access the service. The user doesn't enter the standard security token.</p>
Call Center	The name of the call center to which this user is assigned.
Checkout Enabled	<p>Indicates whether the user is notified by email when the user's Checkout account is activated and available for login.</p> <p>Enabling this option requires the Manage Billing permission.</p>
City	City portion of user's address. Up to 40 characters are allowed in this field.

Field	Description
Color-Blind Palette on Charts	Indicates whether the option to set an alternate color palette for charts has been enabled. The alternate palette has been optimized for use by users who want high-contrast. For dashboard emails, the alternate palette isn't used.
Company	Company name where user works. Up to 40 characters are allowed in this field.
Contact	Name of the associated contact if the user is a partner user.
Country	Country portion of user's address. Entry is selected from a picklist of standard values, or entered as text. Up to 80 characters are allowed if the field is a text field.
Created By	User who created the user including creation date and time. (Read only)
Currency	User's default currency for quotas, forecasts, and reports. Shown only in orgs using multiple currencies. This currency must be one of the active currencies for the org.
Custom Links	Listing of custom links for users as set up by your administrator.
Data.com User Type	Enables a user to find contact and lead records from Data.com and add them to Salesforce. Also indicates the type of Data.com user. Data.com Users get a limited number of account, contact, and lead records to add or export per month, and their unused additions expire at the end of each month. Data.com List Users get a limited number of account, contact, and lead records to add or export per month, and their unused additions expire at the end of each month. After the monthly limit is used, List Users draw record additions from a pool that is shared by all List Users in the organization. Unused pool additions expire one year from purchase.
Default Currency ISO Code	User's default currency setting for new records. Available only for orgs that use multiple currencies.
Default Division	<p>Division that is applied, by default, to all new accounts and leads created by the user, unless the user explicitly sets a different division. When users create records related to an account or other record that already has a division, the new record is assigned to the existing record's division. The default division isn't used.</p> <p>This setting doesn't restrict the user from viewing or creating records in other divisions. Users can change their default division at any time by setting a working division.</p> <p>Available only in orgs that use divisions to segment their data.</p>
Delegated Approver	User lookup field used to select a delegate approver for approval requests. Depending on the approval process settings, this user can also approve approval requests for the user.

Field	Description
Department	Group that user works for, for example, Customer Support. Up to 80 characters are allowed in this field.
Development Mode	Enables development mode for creating and editing Visualforce pages. This field is visible only to orgs that have Visualforce enabled.
Disable Auto Subscription For Feeds	Disables automatic feed subscriptions to records owned by a user. Only available in orgs with Chatter enabled.
Division	Company division to which user belongs for example, PC Sales Group. Up to 40 characters are allowed in this field.
Email	Email address of user. Must be a valid email address in the form: jsmith@acme.com. Up to 128 characters are allowed in this field.
Email Encoding	Character set and encoding for outbound email sent by user from within Salesforce. English-speaking users use ISO-8859-1, which represents all Latin characters. UTF-8 (Unicode) represents characters for all languages, however some older email software doesn't support it. Shift_JIS, EUC-JP, and ISO-2022-JP are useful for Japanese users.
Employee Number	Identifying number for a user.
End of day	Time of day that user generally stops working. Used to define the times that display in the user's calendar.
Fax	Fax number for user.
Federation ID	The value used to identify a user for federated authentication single sign-on.
First Name	First name of user, as displayed on the user edit page. Up to 40 characters are allowed in this field.
Flow User	Grants the ability to run flows. Available in Developer (with limitations), Enterprise, Unlimited, and Performance Editions. Enabling this option requires the Manage Flow permission. If the user has the Run Flows permission, don't enable this field.
Lightning Platform Quick Access Menu	Enables the Lightning Platform quick access menu, which appears in object list view and record detail pages. The menu provides shortcuts to customization features for apps and objects.
Information Currency	The default currency for all currency amount fields in the user record. Available only for orgs that use multiple currencies.
Knowledge User	Grants access to Salesforce Knowledge. The user's profile determines whether the user has access to the Article Management tab or Articles tab. Available in Professional, Enterprise, Unlimited, and Performance Editions.

Field	Description
Language	<p>The primary language for the user. All text and online help is displayed in this language. In Professional, Enterprise, Unlimited, and Performance Edition orgs, a user's individual Language setting overrides the org's Default Language.</p> <p>Not available in Personal Edition, Contact Manager, or Group Edition™. The org's Display Language applies to all users.</p>
Last Login	<p>The date and time when the user last successfully logged in. This value is updated if 60 seconds have elapsed since the user's last login. (Read only)</p>
Last Name	<p>Last name of user, as displayed on the user edit page. Up to 80 characters are allowed in this field.</p>
Last Password Change or Reset	<p>The date and time of this user's last password change or reset. This read-only field appears only for users with the Manage Users permission.</p>
Lightning Login	<p>Allows the user to enroll in and use Lightning Login, for password-free logins. The Enroll option indicates that a Salesforce admin has given the user the option to enroll. The Cancel option indicates that the user has enrolled, and can cancel their enrollment if needed.</p>
Locale	<p>Country or geographic region in which user is located.</p> <p>The <code>Locale</code> setting affects the format of date, date/time, and number fields, and the calendar. For example, dates in the English (United States) locale display as 06/30/2000 and as 30/06/2000 in the English (United Kingdom) locale. Times in the English (United States) locale display using a twelve-hour clock with AM and PM (for example, 2:00 PM), whereas in the English (United Kingdom) locale, they're displayed using a 24-hour clock (for example, 14:00). The user's <code>Language</code> setting determines the language of the AM/PM designator in date/time fields. For example, if the user's language is English, times in the Chinese (Singapore) locale display with English AM/PM designators.</p> <p>The <code>Locale</code> setting also affects the first and last name order on <code>Name</code> fields for users, leads, and contacts. For example, Bob Johnson in the English (United States) locale displays as Bob Johnson, whereas the Chinese (China) locale displays the name as Johnson Bob.</p> <p>For Personal Edition users, the locale is set at the org level (from Setup, enter <i>Company Information</i> in the Quick Find box, then select Company Information). For all other users, their personal locale, available at their personal information page, overrides the org setting.</p>

Field	Description
Make Setup My Default Landing Page	When this option is enabled, users land in the Setup page when they log in.
Manager	<p>Lookup field used to select the user's manager. This field:</p> <ul style="list-style-type: none"> • Establishes a hierarchical relationship, preventing you from selecting a user that directly or indirectly reports to itself. • Allows Chatter to recommend people and records to follow based on your org's reporting structure. <p>This field is especially useful for creating hierarchical workflow rules and approval processes without creating more hierarchy fields.</p> <p>Unlike other hierarchy fields, you can inactivate users referenced in the Manager field.</p>
Marketing User	<p>When enabled and the user has Read permission on contacts or the Import permission on Leads, and Edit permission on campaigns, the user can create, edit, and delete campaigns, configure advanced campaign setup, and add campaign members and update their statuses with the Data Import Wizard. Available in Professional, Enterprise, Unlimited, and Performance Editions.</p> <p>If this option isn't selected, or the user doesn't have the necessary permissions, the user can only view campaigns and advanced campaign setup, edit the Campaign History for a single lead or contact, and run campaign reports.</p>
Middle Name	<p>Middle name of the user, as displayed on the user edit page. Up to 40 characters are allowed for this field.</p> <p>To enable this field, from Setup, enter <i>User Interface</i> in the Quick Find box, then select User Interface. In Lightning Experience, the User Interface page is the last item under the User Interface node. Then select Enable Middle Names for Person Names.</p>
Mobile	<p>Cellular or mobile phone number. Up to 40 characters are allowed in this field.</p> <p>This number is used for SMS-based device activation. Administrators enable SMS-based device activation from Setup by entering <i>Session Settings</i> in the Quick Find box, then selecting Session Settings, and then selecting the Enable the SMS method of device activation option.</p> <p>After the SMS method of device activation is enabled, users without a verified mobile number in their profiles are asked after logging in to register for mobile verification. This process applies to users without mobile numbers. Users can take one of the following actions. After a user's mobile phone number is verified, Salesforce</p>

Field	Description
	<p>uses it to authenticate the user when necessary. For example, verification occurs when a user logs in from an unknown IP address.</p> <ul style="list-style-type: none"> • Enter a mobile phone number and then have it verified with a text message containing a verification code. • Skip entering a mobile number now, but be asked again at the next login. • Opt out of mobile verification. Users who select this action can register a mobile number later in their personal information. Chatter Free and Chatter External license users who select this action need an administrator to set the mobile number. <p>Administrators can also enter users' mobile numbers and pre-verify them. If Enable the SMS method of device activation is enabled when an administrator enters a mobile number for a user, or when a mobile number is set from an API using the <code>User</code> object, the mobile number is considered verified. If Enable the SMS method of device activation isn't enabled, the new mobile phone number isn't considered verified.</p>
Mobile Configuration	<p>The mobile configuration assigned to the user. If no mobile configuration is specified, this field defaults to the mobile configuration assigned to the user's profile.</p> <p>This field is visible to orgs that use Salesforce to manage mobile configurations.</p>
Modified By	User who last changed the user fields, including modification date and time. (Read only)
Monthly Contact and Lead Limit	<p>If the user's Data.com User Type is Data.com User, the number of Data.com contact and lead records the user can add each month.</p> <p>The default number of records per license is 300, but you can assign more or fewer, up to the org limit.</p>
Name	Combined first name, middle name (beta), last name, and suffix (beta) of user, as displayed on the user detail page.
Nickname	A nickname is the name used to identify this user in an Experience Cloud site. Up to 40 alphanumeric characters are allowed. Standard users can edit this field.
Offline User	Administrative checkbox that grants the user access to Connect Offline. Available in Professional, Enterprise, Unlimited, and Performance Editions.
Partner Super User	Denotes whether a partner portal user is a super user.
Phone	Phone number of user. Up to 40 characters are allowed in this field.

Field	Description
Profile	Administrative field that specifies the user's base-level permissions to perform different functions within the application. You can grant more permissions to a user through permission sets.
Receive Approval Request Emails	Preference for receiving approval request emails. This preference also affects whether the user receives approval request notifications in the Salesforce mobile app or Lightning Experience.
Receive Salesforce CRM Content Daily Digest	Specifies that non-portal users with a Salesforce CRM Content User license and Salesforce CRM Content subscription receive a daily email summary if activity occurs on their subscribed content, libraries, tags, or authors. To receive email, you must also select the <code>Receive Salesforce CRM Content Email Alerts</code> option. Portal users don't need the Salesforce CRM Content User license. They need only the <code>View Content in Portals</code> user permission.
Receive Salesforce CRM Content Email Alerts	Specifies that non-portal users with a Salesforce CRM Content User license and Salesforce CRM Content subscription receive email notifications if activity occurs on their subscribed content, libraries, tags, or authors. To receive real-time email alerts, select this option and don't select the <code>Receive Salesforce CRM Content Daily Digest</code> option. Portal users don't need the Salesforce CRM Content User license. They need only the <code>View Content in Portals</code> user permission.
Role	Administrative field that specifies position of user within an organization, for example, Western Region Support Manager. Roles are selected from a picklist of available roles, which the administrator can change. Users with the <code>View Roles and Role Hierarchy</code> permission can view role information. Not available in Personal Edition, Contact Manager, or Group Edition.
Salesforce CRM Content User	Indicates whether a user can use Salesforce CRM Content. Available in Professional, Enterprise, Unlimited, and Performance Editions.
Self-Registered via Customer Portal	When enabled, specifies that the user was created via self-registration to a Customer Portal. Available in Enterprise, Unlimited, and Performance Editions.
Security Key (U2F)	Allows the user to register and use a U2F-compatible security key as a second factor of authentication. The Register option indicates that a Salesforce admin has given users in the org the option to register a security key. The Remove option indicates that the user has registered a security key, and can remove their registration if needed.

Field	Description
Send Apex Warning Emails	<p>Specifies that users receive an email notification whenever they execute Apex that surpasses more than 50 percent of allocated governor limits.</p> <p>Available in Developer, Enterprise, Unlimited, and Performance Editions only.</p>
Show View State in Development Mode	<p>Enables the View State tab in the development mode footer for Visualforce pages.</p> <p>This field is only visible to orgs that have Visualforce enabled and Development Mode selected.</p>
Site.com Contributor User	<p>Allocates one Site.com Contributor license to the user, granting the user limited access to Site.com Studio. Users with a Contributor license can use Site.com Studio to edit site content only.</p> <p>The number of user records with this checkbox enabled can't exceed the total number of Site.com Contributor licenses your org has.</p> <p>Available in Developer, Enterprise, Unlimited, and Performance Editions, only if Site.com is enabled for your org.</p>
Site.com Publisher User	<p>Allocates one Site.com Publisher license to the user, granting the user full access to Site.com Studio. Users with a Publisher license can build and style websites, control the layout and functionality of pages and page elements, and add and edit content.</p> <p>The number of user records with this checkbox enabled can't exceed the total number of Site.com Publisher licenses your org has.</p> <p>Available in Developer, Enterprise, Unlimited, and Performance Editions, only if Site.com is enabled for your org.</p>
Start of day	<p>Time of day that user generally starts working. Used to define the times that display in the user's calendar.</p>
State/Province	<p>State or province portion of user's address. Entry is selected from a picklist of standard values, or entered as text. Up to 80 characters are allowed if the field is a text field.</p>
Suffix	<p>Name suffix of the user, as displayed on the user edit page. Up to 40 characters are allowed for this field.</p> <p>To enable this field, from Setup, enter <i>User Interface</i> in the Quick Find box, then select User Interface. In Lightning Experience, the User Interface page is the last item under the User Interface node. Then select Enable Name Suffixes for Person Names.</p>

Field	Description
Temporary Verification Code	Users can enter a temporary code when they forget or lose the verification method that they usually use for multi-factor authentication. Only Salesforce admins can generate or expire a temporary code for a user. Users can expire their own code.
Time Zone	Primary time zone in which user works. Users in Arizona select the setting with America/Phoenix , and users in parts of Indiana that don't follow Daylight Savings Time select the setting with America/Indianapolis .
Title	Job title of user. Up to 80 characters are allowed in this field.
Used Space	Amount of disk storage space the user is using.
User License	Indicates the type of user license.
Username	Administrative field that defines the user's login. Up to 80 characters are allowed in this field.
Zip/Postal Code	ZIP code or postal code portion of user's address. Up to 20 characters are allowed in this field.

SEE ALSO:

[View and Manage Users](#)

[User Licenses](#)

[View Your Organization's Feature Licenses](#)

[Restrict User Email Domains](#)

Licenses Overview

To enable specific Salesforce functionality for your users, you must choose one user license for each user. To enable more functionality, you can assign permission set licenses and feature licenses to your users or purchase usage-based entitlements for your organization.

For example, to view contracts, a user must have the Read permission on contracts. To assign a given permission to a user, that user's license (or licenses) must support the permission. Multiple licenses can support a single permission.

Think of permissions as locks and of licenses as rings of keys. Before you can assign users a specific permission, they must have a license that includes the key to unlock that permission. Although every user must have exactly one user license, you can assign one or more permission set licenses or feature licenses to incrementally unlock more permissions.

Continuing our example, the Salesforce user license includes the key to unlock the Read permission on contracts. The Chatter Free user license doesn't. If you try to assign that permission to a Chatter Free user, you get an error message.

You can view your Salesforce org's licenses on the Company Information page in Setup. To learn how to check your remaining licenses, watch [How Many Licenses Have I Used? \(English Only\)](#). You can also track the number of active user licenses, permission set licenses, and feature licenses with the Active Licenses tab in the [Lightning Usage App](#).

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Edition requirements vary for each user, permission set, and feature license type.

Salesforce provides these types of licenses and usage-based entitlements.

[User Licenses](#)

A user license determines the baseline of features that the user can access. Every user must have exactly one user license. You assign user permissions for data access through a profile and optionally one or more permission sets.

[Permission Set Licenses](#)

Permission set licenses entitle users to access additional features not included in their assigned user license. Users can be assigned any number of permission set licenses.

[Feature Licenses Overview](#)

A feature license entitles a user to access an additional feature that isn't included with his or her user license, such as Marketing or WDC. Users can be assigned any number of feature licenses.

[Usage-Based Entitlements](#)

A usage-based entitlement is a limited resource that your organization can use on a periodic basis. For example, the allowed number of monthly logins to a Partner Community or the record limit for Data.com list users are usage-based entitlements.

User Licenses

A user license determines the baseline of features that the user can access. Every user must have exactly one user license. You assign user permissions for data access through a profile and optionally one or more permission sets.

Assign licenses for your users' job functions, so that they're entitled the permissions required for their day-to-day tasks. For example:

- Employee A needs access to custom apps, but not the full CRM functionality. Assign Employee A a Lightning Platform user license, which supports standard object permissions for accounts and contacts, but not cases.
- Employee B needs full access to standard CRM apps and objects. Assign Employee B a Salesforce user license, which allows you to grant them standard object permissions for accounts, contacts, and cases.

You assign licenses to users when they're added to your org. You can change a user's license on their User Detail page. Changing a user's license also removes any permission sets and permission set licenses that are assigned to the user.

User licenses offered by Salesforce include:

- [Standard User Licenses](#)
- [Chatter User Licenses](#)
- [Experience Cloud User Licenses](#)
- [Service Cloud Portal User Licenses](#)
- [Sites and Site.com User Licenses](#)
- [Authenticated Website User Licenses](#)

To purchase user licenses, contact your Salesforce account representative. Your Salesforce org can also have other licenses that are supported but no longer available for purchase.

SEE ALSO:

[View Your Organization's User Licenses](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Edition requirements vary for each user license type.

View Your Organization's User Licenses

View the user licenses that your company has purchased to know what you have available to assign to your users.

To learn how to check your remaining licenses, watch [▶ How Many Licenses Have I Used? \(English Only\)](#).

1. From Setup, enter *Company Information* in the **Quick Find** box, then select **Company Information**.
2. See the User Licenses related list.

For information on purchasing user licenses, contact your Salesforce account representative.

SEE ALSO:

[User Licenses](#)

[See User License Assignments with a Custom Report Type](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

USER PERMISSIONS

To view user licenses:

- [View Setup and Configuration](#)

See User License Assignments with a Custom Report Type

Create a custom report type to report on which user licenses your users are assigned.

For a video walk-through of these steps, watch [▶ Track your Salesforce Users and Licenses with Custom Report Types \(English Only\)](#).

1. Create a custom report type with **Users** as the primary object.
2. To configure the field layout of reports created from this custom report type, click **Edit Layout**.
3. Click **Add fields related via lookup**.
4. Click **Profile**, then select **User License**. Click **view related fields...** and select any additional fields, such as Expiration Date, Status, Total Licenses, and Usage Type. Click **OK**.
5. Click **Save**.
6. [Build a Report](#) with the custom report type that you created.
7. In the left panel, add the related fields that you want displayed in your report. To group by user license, under Group Rows, select the **Profile: User License: Name** field.
8. In the left panel, under Filters, if you see a filter for Chatter Adoption Stage Modified Date, change the range to **All Time**.

We recommend that you filter out users that aren't assigned a license, such as automated users.

You can see permission set license assignments on the Company Information page. For more information, see [View and Manage Your Permission Set Licenses](#).

SEE ALSO:

[View Your Organization's User Licenses](#)

Standard User Licenses

Find information about standard user licenses that you can get for your org, such as the Salesforce and Lightning Platform user licenses.

To purchase user licenses, contact your Salesforce account representative.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To create and update custom report types and to create, edit, and delete reports:

- **Legacy Folder Sharing**
Create and Customize Reports
AND
Manage Custom Report Types
- **Enhanced Folder Sharing**
Create and Customize Reports
AND
Manage Custom Report Types

To view license information:

- View Setup and Configuration

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Edition requirements vary for each user license type.

License Type	Description	Available in
Salesforce	<p>Designed for users who require full access to standard CRM and AppExchange apps. Users with this user license are entitled to access any standard or custom app.</p> <p>Each license provides more storage for Enterprise, Unlimited, and Performance Edition users.</p>	All editions
Knowledge Only User	<p>Designed for users who only need access to the Salesforce Knowledge app. This license provides access to custom objects, custom tabs, and the following standard tabs.</p> <ul style="list-style-type: none"> Articles Article Management Chatter Files Home Profile Reports Custom objects Custom tabs <p>The Knowledge Only User license includes a Knowledge Only profile that grants access to the Articles tab. To view and use the Article Management tab, a user must have the Manage Articles permission.</p> <p>To view articles, a user must have the AllowViewKnowledge permission on their profile. But this permission is off for default profiles. To give a user the AllowViewKnowledge permission on their profile, activate the permission on a cloned profile and assign the cloned profile to the user.</p>	Enterprise, Unlimited, and Performance Editions
Identity Only	<p>Provides extra licenses for employees to access only identity services, such as single sign-on (SSO). For example, some of your employees don't need access to all the solutions included with a Salesforce license. But you want these employees to be able to sign in to a custom Your Benefits web app directly from your Salesforce org using SSO. You can purchase the Identity Only license for them. This license provides access to the same identity services that are included with your other paid licenses in the Enterprise, Unlimited, Performance, and Developer Editions.</p> <p>For more information about Salesforce identity services, see Identify Your Users and Manage Access.</p>	<p>Enterprise, Unlimited, Performance, and Developer Editions</p> <p>Ten free Identity user licenses are included with each new Developer Edition org.</p>
External Identity	<p>Grants access to Salesforce Customer Identity, which enables customers and partners to self-register, log in, update their profile, and securely access web and mobile apps with a single identity. Plus, you can customize Customer Identity to your specific business process and brand using the power of the Salesforce Platform. For more information, see External Identity License Details and Salesforce Identity Licenses.</p>	<p>Enterprise, Unlimited, Performance, and Developer Editions</p> <p>Five free External Identity user licenses are included with each new Developer Edition org.</p>

License Type	Description	Available in
Salesforce Integration	<p>Grants access to Salesforce data and features only through the API. This license is designed for system-to-system integrations. It can't be used for human users that need to access Salesforce data or features through any user interface.</p> <p>For more information, see Give Integration Users API Only Access.</p>	<p>Enterprise, Unlimited, Performance, and Developer Editions</p> <p>Five Salesforce Integration user licenses are included in each Enterprise, Unlimited, and Performance Edition org. One Salesforce Integration license is included in each Developer Edition org.</p>
WDC Only User	<p>Designed for users who don't have a Salesforce license and need access to WDC.</p> <p> Note: Chatter must be enabled for WDC features to fully function.</p>	<p>Professional, Enterprise, Unlimited, Performance, and Developer Editions</p>

Lightning Platform User License Types

License type	Description	Available in
Salesforce Platform	<p>Designed for users who need access to custom apps but not to standard CRM functionality. Users with this user license are entitled to use custom apps developed in your organization or installed from AppExchange. Plus, they're entitled to use core platform functionality such as accounts, contacts, reports, dashboards, documents, and custom tabs. These users aren't entitled to some user permissions and standard apps, including standard tabs and objects such as forecasts, leads, campaigns, and opportunities. Users with this license can also use Connect Offline.</p> <p>Users with a Salesforce Platform user license can access all the custom apps in your organization.</p> <p>Each license provides more storage for Enterprise, Unlimited, and Performance Edition users.</p> <p>To view articles, a user must have the AllowViewKnowledge permission on their profile. But this permission is off for default profiles. To give a user the AllowViewKnowledge permission on their profile, activate the permission on a cloned profile and assign the cloned profile to the user.</p>	<p>Enterprise, Unlimited, Performance, and Developer Editions</p>
Lightning Platform - One App	<p>This license isn't available for new customers.</p> <p>Designed for users who need access to one custom app but not to standard CRM functionality. Lightning Platform - One App users are entitled to most of the same rights as Salesforce Platform users, plus they have access to an unlimited number of custom tabs. But they're limited to one custom app, which is defined as up to 10 custom objects. They're also limited to</p>	<p>Enterprise and Unlimited Editions</p>

License type	Description	Available in
	<p>read-only access of the Accounts and Contacts objects. Push Topic object read permission isn't available.</p> <p>Users with this license can only view dashboards if the running user also has the same license.</p> <p>Each license provides an extra 20 MB of data storage and 100 MB of file storage, regardless of the Salesforce edition.</p> <p>To view articles, a user must have the AllowViewKnowledge permission on their profile. But this permission is off for default profiles. To give a user the AllowViewKnowledge permission on their profile, activate the permission on a cloned profile and assign the cloned profile to the user.</p>	
Force.com - App Subscription	<p>Grants users access to a Lightning Platform Light App or Lightning Platform Enterprise App. CRM functionality isn't included.</p> <p>A Lightning Platform Light App has up to 10 custom objects and 10 custom tabs, has read-only access to accounts and contacts, and supports object-level and field-level security. A Lightning Platform Light App can't use the Bulk API or Streaming API.</p> <p>A Lightning Platform Enterprise App has up to 10 custom objects and 10 custom tabs. It has the permissions of a Lightning Platform Light App, plus it supports record-level sharing, can use the Bulk API and Streaming API, and has read/write access to accounts and contacts.</p> <p>Assign users with this license a profile or permission set that allows access only to 10 custom objects and 10 custom tabs.</p> <p>Users with this license can only view dashboards if the running user also has the same license.</p> <p>Each license provides 20 MB more data storage per user for Enterprise Edition and 120 MB more data storage per user for Unlimited and Performance Editions, as well as 2 GB of file storage regardless of the edition.</p> <p>To view articles, a user must have the AllowViewKnowledge permission on their profile. But this permission is off for default profiles. To give a user the AllowViewKnowledge permission on their profile, activate the permission on a cloned profile and assign the cloned profile to the user.</p>	Enterprise, Unlimited, and Performance Editions
Company Community User	<p>This license is an internal user license for employee communities. It's designed for users to access custom tabs, Salesforce Files, Chatter (people, groups, feeds), and an Experience Cloud site.</p> <p>Company Community users have read-only access to Salesforce Knowledge articles. They can also:</p> <ul style="list-style-type: none"> • Access up to 10 custom objects and 10 custom tabs • Use Content, Ideas, Assets, and Identity features • Use activities, tasks, calendar, and events • Have access to accounts, contacts, cases, and documents. 	Enterprise, Unlimited, Performance, and Developer Editions

License type	Description	Available in
Developer	<p>Designed for users whose role is to build customizations or applications. This license provides access to development tools and environments. It comes with one Developer sandbox, one scratch org, and access to the Dev Hub. In the production org, this license restricts access to standard and custom objects. For example, users can't access the Account object within the Sales app. And because of the restriction to custom objects, users can't be assigned access to custom apps or AppExchange apps.</p> <p>The development environments provide access to Salesforce features. With a Developer sandbox, you can use all the features that exist in the production org. The org administrator can create the Developer sandbox that was provisioned with the Developer license. A scratch org, which can be configured to your specifications using a scratch org definition file, gives you access to features on a trial basis. For example, you can use a scratch org to work with Financial Services Cloud or to play with Sales Cloud Einstein features. The Developer license provides access to the Dev Hub, enabling users to create scratch orgs on a self-service basis.</p>	Enterprise, Unlimited, and Performance Editions

SEE ALSO:[User Licenses](#)[View Your Organization's User Licenses](#)**When to Use an Internal or External License**

The Salesforce platform supports multiple use cases and stakeholders, such as employees, partners, brokers, and end customers. To account for the differences in features, user experiences, sharing requirements, data security, and other needs for the various roles, Salesforce has built purpose-driven applications and licenses. Learn about the various use cases and available licenses to make informed license purchasing decisions.

See the different Salesforce user types in action in the video, [Internal, External, and Guest Users in Salesforce](#).

What Is an Internal User and Internal License?

An internal user logs in to Salesforce via `login.salesforce.com` or a company-specific My Domain login URL, like `acme.my.salesforce.com`, using an internal license. Internal users primarily access the Salesforce platform using Lightning Experience or Salesforce Classic. Internal users can also access Experience Cloud sites.

What Is an External User and External License?

Salesforce customers who want to create an experience connected to their CRM data for their end customers, prospects, partners, brokers, dealers, and other external stakeholders use external licenses to provide access. Some typical use cases are partner portals, self-service forums and help centers, customer portals, and broker and dealer portals. A user with an external license can access only the Experience Cloud sites that the user is a member of. An external user can't access the internal Lightning Experience or Salesforce Classic.

For example, Acme Insurance is a Salesforce customer. Acme employees have internal licenses and log in to Salesforce. Acme created a broker portal for its partners with the URL `partners.acme.com`. When Acme brokers log in to `partners.acme.com` with an

EDITIONS

Available in: Salesforce Classic (**not available in all orgs**) and Lightning Experience

Edition requirements vary for each user license type.

external license, they're not aware that they're using Salesforce. Instead, the Acme portal is a secure space just for Acme brokers, not for Acme employees.

When Do Salesforce Customers Use Internal Licenses?

Anyone who is an employee of a company or needs employee privileges requires an internal license. For example, Acme Insurance uses Salesforce as its CRM. The Acme sales and service teams, who are full-time employees, need an internal license to log in to Salesforce to do their day-to-day work.

Acme uses consultants to take care of the company's Salesforce setup and administration. The consultants also need internal licenses, even though they aren't Acme employees. Other users who need an internal license to the Acme org are the company's accountants and lawyers, who also work for other companies, to access the company's information. The key point is that you're treating all these users as employees. Acme is granting the same privileges to employees and consultants and is fine with the broader data and permission access.

When Do Customers Use External Licenses?

Use external licenses for anyone outside your company who you want to:

- Limit access to your data
- Restrict privacy or security and sharing considerations
- Provide a more limited set of permissions (for example, can't manage other users in the org or have access to modify all data)
- Limit access to a subset of information that is contained in your org

For example, a broker could need access only to a subset of information in your org. Acme has an internal sales team, but it also has independent brokers who sell Acme products. The brokers need to access leads and opportunities, but they don't need to see the company's internal Chatter feeds or cases.

Other examples of Acme users who could need external licenses are:

- End customers (that is, customers of Acme)
- System integrators
- Franchisees
- Resellers
- Distributors
- Wholesalers
- Retailers
- Agents
- Dealers
- Anyone in the Acme sphere who isn't an employee

These Experience Cloud licenses are only to be used by external users. Don't assign them to internal employees or contractors.

- External Apps
- External Apps Login
- Channel Account
- Customer Community
- Customer Community Login
- Customer Community Plus
- Customer Community Plus Login
- Partner Community
- Partner Community Login

Why Not Use Internal Licenses for External Use Cases?

Internal licenses provide broader access to your company data and information. The incorrect use of an internal license for an external use case can provide external users unwanted or inappropriate access to your data and records.

Internal license types are built with one use case in mind: a company employee or consultant that needs access to company data in the Salesforce org.

External license types are created for a multitude of use cases and include [an added security](#) level not available with internal licenses.

The best practice for any org is to use external licenses for external use cases, and internal licenses for internal use cases.

SEE ALSO:

[Standard User Licenses](#)

[Experience Cloud User Licenses](#)

External Identity License Details

Salesforce Customer Identity is available when you purchase the External Identity license. You can purchase the External Identity license in blocks of active users. These users are typically consumers of your business, such as customers, purchasers, patients, partners, and dealers.

With Customer Identity, customers and partners can self-register, log in, update their profile, and securely access web and mobile apps with a single identity. Plus, Customer Identity is customized to your specific business process and brand using the power of the Salesforce Platform. And you can use the product to store and manage customer and partner user records and to authenticate these users in several ways.

The External Identity license works with Community licenses. It's also included for free with all paid Community user licenses in Enterprise, Performance, and Unlimited Editions. Each Developer Edition org includes five External Identity user licenses. You can upgrade the External Identity license to a Community license to benefit from Experience Cloud features, including Cases, Contracts, Notes, Orders, and Tasks. The External Identity license requires unique usernames within the Salesforce org that an Experience Cloud site belongs to.

We recommend that the number of External Identity license users in your Experience Cloud site not exceed 10 million unique logins per month. If you require user licenses beyond this limit, contact your Salesforce representative. Exceeding this limit can result in an extra charge and decrease expected functionality.

External Identity User Profile

When you purchase the External Identity license to enable access to Customer Identity, you also get access to the External Identity User profile. This profile defines a set of object permissions that you can assign to a customer or partner. It also defines a default External Identity User profile, which contains a more limited set of object permissions. For example, with the default profile, users can read accounts. With the full license, users can read and update accounts.

You can increase object access by cloning the default profile and changing object permissions as needed.

 **Note:** The default External Identity User profile is limited to avoid unintended data leaks. This stricter default profile applies to users assigned to this profile as of Spring '19 and applies only to new Salesforce orgs. Users provisioned before Spring '19 aren't affected.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

External Identity licenses are available in: **Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To assign and manage customers and partners:

- Manage Users

To enable Experience Cloud sites:

- Customize Application

Salesforce Standard Objects

With an External Identity license, you can access several standard objects and 10 custom objects to deliver powerful self-service applications. The license includes extra data storage and API requests. Make sure that your org has sufficient resources before rolling out your Customer Identity configuration. This table lists all the object permissions that you can assign to customers and partners, and which ones are available with the default license.

	Create	Read	Update	Delete	Default Profile
Accounts		✓	✓		Read
AccountBrands	✓	✓	✓	✓	Not Available
Accreditations	✓	✓	✓		Not Available
Addresses		✓			Not Available
Assets	✓	✓	✓		Create, Read, Update
Contacts	✓	✓	✓		Read, Update
Documents		✓			Read
Household	✓	✓	✓		Not Available
Individuals	✓	✓	✓		Read, Update
Location		✓			Not Available
Party-Related Party	✓	✓	✓		Not Available
Party Relationship	✓	✓	✓		Not Available
Plan Benefit		✓			Not Available
Plan Benefit Item		✓			Not Available
Questions	✓	✓			Not Available

Salesforce Features, Custom Objects, and Storage

Chatter	People, Groups, Feeds, and Private Messages
Files	<ul style="list-style-type: none"> • 2 GB when uploaded via the web interface • 100 MB when uploaded from a mobile device
Custom Objects	Ten custom objects per profile, but custom objects in managed packages don't count toward this limit
Additional Storage	<ul style="list-style-type: none"> • 150 MB—25,000 active users • 2 GB—250,000 active users • 10 GB—1,000,000 active users • 60 GB—5,000,000 active users

Chatter User Licenses

All standard Salesforce licenses allow free Chatter access for everyone in your organization. Salesforce also offers Chatter-specific licenses: Chatter External, Chatter Free, and Chatter Only (also known as Chatter Plus). The Chatter Only license is available for purchase only by existing Chatter Plus customers. For new customers, the Lightning Platform Starter license is a step up from Chatter Only, giving your users access to a more robust set of features.

Chatter External

This license is for users who are outside of your company's email domain. These external users, also called customers, can be invited to Chatter groups that allow customers. Customers can access information and interact with users only in the groups they're invited to. They have no access to Chatter objects or data. Chatter External users can view user profiles, but they can't edit them.

Chatter Free

The Chatter Free license is for users who don't have Salesforce licenses but must have access to Chatter. These users can access standard Chatter items such as people, profiles, groups, and files, but they can't, for security reasons, access any Salesforce objects or data. For example, Chatter Free users can't be attendees at events created in Salesforce. Chatter Free users can be Chatter moderators.

Chatter Free users don't see tabs like other Salesforce users. Chatter Free users access feeds, people, groups, and files using the App Launcher in Lightning Experience. In Salesforce Classic, users access these features from links in the page sidebar.

Salesforce administrators can upgrade a Chatter Free license to a standard Salesforce or Lightning Platform Starter license at any time. You can't convert a standard Salesforce, Lightning Platform Starter, or Chatter Only license to a Chatter Free license.

Chatter Only (Chatter Plus)

The Chatter Only license is also known as the Chatter Plus license. It's available only to existing Chatter Plus customers. The Chatter Plus license is for users who don't have Salesforce licenses but must have access to Chatter and some additional Salesforce objects. Chatter Plus users can be Chatter moderators and have access to standard Chatter people, profiles, groups, and files pages. They can also

- View Salesforce accounts and contacts
- Use Salesforce CRM Content, Ideas, and Answers
- Access dashboards and reports
- Use and approve workflows
- Use the calendar to create and track activities
- View and modify up to 10 custom objects
- Add records to groups

If you're an existing Chatter Plus customer, you can buy more Chatter Plus licenses, or you can upgrade to Lightning Platform Starter.

By default, the tabs for standard Salesforce objects are hidden from Chatter Plus users. Expose these tabs if you want to make them available to Chatter Plus users. For more information on Chatter Plus users, see [Chatter Plus Frequently Asked Questions](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Chatter External and Chatter Free licenses are available in: **Group, Professional, Enterprise, Performance, Unlimited, Contact Manager, and Developer** Editions

Chatter Only (also known as Chatter Plus) licenses are available in: **Professional, Enterprise Unlimited, and Performance** Editions

Lightning Platform Starter licenses are available in: **Enterprise, Performance, Unlimited, and Developer** editions

Lightning Platform Starter (for Partner and Customer Sites)

The Lightning Platform Starter license is for users in Experience Cloud sites who must have access to Chatter and a wide variety of Salesforce objects. Lightning Platform Starter users can be Chatter moderators and have access to standard Chatter people, profiles, groups, and files pages. They can also interact with

- Accounts
- Assets
- Cases
- Contacts
- Dashboards (read only)
- Documents
- External Objects (Salesforce Connect)
- Events and Calendars
- Ideas
- List Views
- Notes and Attachments
- Reports
- Tasks
- Work Orders
- Work Order Line Items

Besides working with these objects, Lightning Platform Starter users have access to these Salesforce features, capabilities, and custom objects

- 20-MB data storage per user license, and 2-GB file storage per user license
- 200 API calls per day per member for Enterprise Edition or Unlimited Edition orgs
- Direct Messages
- 10 custom objects per license (custom objects in managed packages don't count towards this limit)
- Knowledge (read only)
- Roles and Advanced Sharing
- Salesforce App
- Send Email
- Thanks Badges
- Tokens
- Workflow Approvals

 **Note:** For a detailed look at the benefits associated with a Lightning Platform Starter license, see [Experience Cloud User Licenses](#)

Chatter License Overview

This table shows the list of features that are available for Chatter External, Chatter Free, Chatter Only, and Lightning Platform Starter licenses.

Feature	Chatter External (Access limited to items and people in the groups customers are invited to)	Chatter Free	Chatter Only (a.k.a. Chatter Plus)	Lightning Platform Starter
Chatter Desktop client	✓	✓	✓	✓
Use the Salesforce mobile app (Downloadable apps require the "API Enabled" profile permission)	✓ Downloadable app users can't access Groups or People list views.	✓	✓	✓
Feeds	✓	✓	✓	✓
File sharing	✓	✓	✓	✓
Files Connect			✓	✓
Groups	✓	✓	✓	✓
Invitations to join groups	✓ Only customers who are also group managers can invite Chatter users from groups they have access to or people outside Chatter.	✓	✓	✓
Profiles	✓ Chatter External users can view profiles, but they can't edit them.	✓	✓	✓
Topics and hash tags		✓	✓	✓
Private messages	✓	✓	✓	✓ (Direct Messages)
Global search	✓ Search results include only those items that customers have access to via groups.	✓	✓ Chatter only users have access to reports and dashboards but can't use global search to find them.	✓
Custom objects			✓ Up to 10 custom objects	✓

Feature	Chatter External (Access limited to items and people in the groups customers are invited to)	Chatter Free	Chatter Only (a.k.a. Chatter Plus)	Lightning Platform Starter
Accounts and contacts			✓ Read only	✓
Calendar and events			✓	✓
Content library			✓	✓
Ideas and answers			✓	✓
Reports and dashboards			✓	✓ (access to dashboards is read-only)
Tasks and activities			✓	✓
Using and approving workflows			✓	✓

Experience Cloud User Licenses

The following licenses are used for external users: Customer Community, Customer Community Plus, Partner Community, External Apps, External Identity, and Channel Account.

Important: Experience Cloud sites use community user licenses.

This topic is intended for Salesforce administrators who want to learn more about the differences between the user licenses intended for external users.

Salesforce packages licenses in specific stock keeping units (SKUs) to sell to customers. SKUs contain one or more licenses and capabilities. Generally, the name of the SKU and the license match, but not always. For example, there are two SKUs that sell the Partner Community license: the Partner Relationship Management SKU and the External Apps SKU. While both SKUs sell the Partner Community license, the External Apps SKU offers more platform capacity in the form of custom objects, file and data storage, and APIs.

After they're purchased, license names (not SKU names) appear in Setup > Company Information.

To learn which SKU and license combination is the best fit for your business needs, contact your Salesforce account executive.

A community license works like a standard Salesforce internal license: external users with a member-based license (that is, a license that is assigned to a specific user) are able to access a community as many times as they want. However, external users don't have access to the internal org.

The External Identity license is a standalone license that you can buy to deliver identity services, like single sign-on and passwordless login, to your customers and partners. To expand user access and capabilities, you can upgrade your External Identity license to a community license at any time. For more information, see [External Identity License Details](#).

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, and Developer** Editions

Frequently Asked Questions About External Licenses

Do I need communities licenses in my org to create Experience Cloud sites?

In Enterprise, Performance, and Unlimited orgs, you can create up to 100 Experience Cloud sites without buying communities licenses. However, you do need to purchase licenses to use specific templates and functionality. For example, to create sites using the Partner Central template, you must purchase at least one Partner Community license. You must have an active community license in your org to use the Archive Site functionality.

You can have up to 100 Experience Cloud sites in your Salesforce org. Active, inactive, and preview sites, including Lightning Platform sites, count against this limit.

Do I need communities licenses in my org to give access to Experience Cloud sites?

There are two types of access to Experiences Cloud sites: authenticated and unauthenticated access. Authenticated users log in to the site, whereas unauthenticated users are considered guest users. Even without community licenses, guest users have some access to your sites (such as to login and error pages). Purchase licenses for external users to allow members to log in or give access to Salesforce objects based on your business needs. Purchasing external licenses also allows you to create external profiles (beyond the guest user profile) to access your sites.

 **Note:** If a community license contract isn't renewed and the license is removed from your org, existing members continue to have access to sites they've been added to. Deactivate sites that you wish to discontinue to ensure security.

If you intend to use your Experience Cloud site as a public knowledge base for unauthenticated users, you don't have to purchase community licenses. For example, guest users can access publicly available Experience Cloud site pages to read knowledge articles.

 **Note:** If your org has legacy portal licenses for authenticated users, you don't have to purchase or convert to community licenses for your authenticated users. You can use legacy portal licenses for sites created with Experience Cloud.

We highly discourage the use of internal licenses for external use cases. External user licenses are the only licenses suited to securely access an external-facing portal or site.

Are community licenses associated with users or a site?

Communities licenses are associated with users, not a specific site. If needed, you can move users with these licenses between sites, and users with community licenses can access multiple sites simultaneously. If you have unused licenses, you can assign them to users in any Experience Cloud site in your org.

Here's another way to think about it: Your Experience Cloud site is like an extension of your Salesforce org that allows users (external and internal) to interact and have selected access to data and functionality. A user's exact access depends on what the license allows.

In addition to supporting communities licenses, Experience Cloud sites support all internal and portal licenses, including existing Customer Portal, Authenticated Website, and partner portal licenses.

Check out [Experience Cloud Sites and Users in Your Salesforce Org](#), a quick video about how Salesforce Experiences live in an org, the differences between licenses, and how Salesforce accounts and site users are associated with one another.

How is a license used in an employee community?

Two underlying licenses support Employee Community licenses—the Salesforce Platform user license and the Company Community for Lightning Platform permission set license. To assign a Lightning Platform Starter or Lightning Platform Plus license to a user, first assign the Salesforce Platform user license. Then assign them the Company Community for Lightning Platform permission set license. (Sometimes, you have to create the permission set before you can assign the license.)

When you upgrade from Lightning Platform Starter license to Lightning Platform Plus license, you get more custom objects, and you don't have to make changes in Setup. [Lightning Platform and Lightning Platform Plus License Details](#) has more about what is included with these licenses.

How are Channel Licenses used?

Channel Licenses are optimized for use with partners, and give you the power to buy a specific number of licenses for your partner accounts. Each partner account with an assigned license is given up to 40 partner users. User licenses are pooled, making it less likely for individual partners to exceed their user limits. More users, beyond the typical 40, can be purchased if necessary.

How do community licenses compare to legacy portal licenses?

Here's a quick correlation of the new communities licenses with their older portal counterparts and their main use case.

 **Important:** Users who have portal licenses can access your site as long as you include them by adding the profiles or permission sets that they're associated with to your site. You don't have to purchase new licenses for them, or swap them for communities licenses.

License Name	Best Used For	Comparable Portal License
External Apps	Custom digital experiences to engage any external stakeholder, including Brand Engagement and Customer Loyalty. Limited access to CRM objects. The External Apps license can be used with person accounts.	High Volume Customer Portal, Service Cloud Portal, Authenticated Sites Portal
Customer Community	Business-to-consumer experiences with large numbers of external users who need access to case objects or knowledge. The Customer Community can be used with person accounts.	High Volume Customer Portal, Service Cloud Portal, Authenticated Sites Portal
Customer Community Plus	Business-to-consumer experiences with external users who need access to reports and dashboards and need standard sharing . The Customer Community Plus can be used with person accounts.	Customer Portal — Enterprise Administration, Customer Portal Manager Standard, Customer Portal Manager Custom
Partner Community	Business-to-business experiences that need access to sales data such as partner relationship management. The Partner Community can't be used with person accounts.	Gold Partner
Channel Account	Business-to-business sites and portals that calculate their usage based on the number of partners instead of the number of individual users.	Gold Partner

 **Note:** Different license types can access your Experience Cloud sites. Your site isn't limited to just one type of license.

What are login-based licenses?

Each community license can be either a member-based license or a login-based license. To use a login-based license, you first purchase a specific number of logins to be used every month. External users associated with that license consume one login each time they log into a site. However, logging in multiple times during the same day still only consumes one login and, after they're logged in, switching between sites doesn't consume extra logins. This type of login is referred to as a daily unique login.

Member-based Licenses	Login-Based Licenses
Customer Community	Customer Community Login
Customer Community Plus	Customer Community Plus Login
Partner Community	Partner Community Login
External Apps	External Apps Login
Channel Account	Channel Account Login

The ratio between the number of monthly logins you purchase and the number of login licenses that are provisioned in your org is 1–20. For example, if you purchase 1,000 monthly logins, then 20,000 login licenses are provisioned in your org. If you want to assign more than 20,000 login licenses, purchase more logins. Why the large ratio? We want to make sure that you have enough licenses to assign to all the login-based users you potentially create.

The timeout period for a session is configurable up to a maximum of 24 hours.

How are login overages calculated?

Login overages are calculated over a 12-month period from the start date of the contract. Entitlements roll over from month to month. If you purchase 1,000 monthly logins, you're entitled to a total of 12,000 annual logins.

In November 2017, we introduced the concept of daily unique logins and beginning on April 1, 2018, they're used to calculate overages.

How can you monitor your login consumption?

You can monitor your login consumption checking the LoginHistory table. In Salesforce Classic, the table is in **Setup > Administer > Manage Users**. In Lightning Experience, **Setup > Identity**.

If you want to check your aggregated login consumption for the current month, use the Usage-based Entitlements list. In Salesforce Classic, find it in **Setup > Administer > Company Information**. In Lightning Experience, it's in **Setup > Company Information**.

Usage-based Entitlement Resource	Description
Customer Community Logins	The number of logins consumed by external users with a Customer Community Login license during the current period.
Power Customer Community Logins	The number of logins consumed by external users with a Customer Community Plus login license during the current period.
Partner Community Logins	The number of logins consumed by external users with a Partner Community Login license during the current period.
External Apps Logins	The number of logins consumed by external users with a External Apps Login license during the current period.

Usage-based Entitlement Resource	Description
Customer Community Daily Unique Logins	The number of unique daily logins consumed by external users with a Customer Community Login license during the current period.
Power Customer Community Daily Unique Logins	The number of unique daily logins consumed by external users with a Customer Community Plus Login license during the current period.
Partner Community Daily Unique Logins	The number of unique logins consumed by external users with a Partner Community Login license during the current period.
External Apps Daily Unique Logins	The number of unique logins consumed by external users with a External Apps login license during the current period.

Is an extra license required to use Experience Builder?

Sites, portals, and communities using a component-based template use Experience Builder to add and edit custom, branded pages. Users with the “Create and Set Up Experiences” permission automatically have full site administrator access to Experience Builder

Do Experience Cloud sites have user or role limits?

For a standard Experience Cloud site, we recommend using the following license types based on the expected number of users.

License Type	Number of Users Per Org
Partner Community, Channel Account, or Customer Community Plus	1+ million
Partner Community, Channel Account, or Customer Community Plus with Account Role Optimization (ARO) ¹	10+ million
Customer Community or External Apps	100+ million

 **Note:** Experience Cloud can support a larger scale of users per org for any of our license types if your community, site, or portal needs more users. To find out if your site needs an in-depth review, consult with your Salesforce account representative. If so, we can provide [performance recommendations](#) to ensure your site scales properly to meet your demands.

Some licenses, such as Customer Community Plus and Partner Community, require roles associated with an external user record. An increase in the number of roles in your org degrades performance, so make sure that you don't use more roles than necessary. The default number of roles used in an org's portals or communities is 50,000. This limit includes roles associated with all of the organization's customer portals, partner portals, or communities. When you reach your portal role limit, you can't create more users. Salesforce emails you when you reach 95% of your limit, so you have time to make adjustments before you run out of roles. To prevent reaching this limit, which can impact performance, review and reduce the number of roles. If you're expecting a high-volume of users, enable account role optimization (ARO). ARO delays the account role creation process until there's a second user on an account, and roles become necessary to support sharing data between them. You can also delete unused roles.

¹ If you're expecting a high-volume of users, we recommend that you enable account role optimization (ARO). From the Spring '22 release onward, ARO optimization is enabled by default for new orgs. You can also enable it for existing orgs.

If you've enabled account role optimization and still require more roles for your site, you can increase the number of roles by designating person account owner power users. Person account owner power users can own a large number of either customer or partner users. They can't change their role, look up to a parent role, or reparent their role. Person account owner power user objects can't be created if deferred sharing is turned on for your org. Create a `PersonAccountOwnerPowerUser` object via API. Enter the user ID of the power user and the type of users that they can own, `Customer` or `Partner`.

 **Note:** Only users at the highest level of a hierarchy can be added to the `PersonAccountOwnerPowerUser` object.

Are guest users counted against my licenses?

Not at all! Unauthenticated or guest users who access your Experience Cloud site don't use up any of your external licenses.

Here are the page view limits for guest users, based on your Salesforce edition. Overages are calculated on a yearly basis. If your growing community exceeds this number of guest user page views, contact your Salesforce account representative to increase your page view limits.

Salesforce Edition	Number of Page Views
Enterprise Edition	500,000/month
Unlimited Edition	One million/month

For example, a site set up in an Enterprise Edition org can have up to 6 million page views over the course of a year. Overages will be calculated after the annual limit has been reached. See [Experience Cloud Site Usage Limits](#) for more information about page view and other user limits.

License Details

By design, the out-of-the-box object permissions of user profiles associated with community licenses are rather restricted. In this table, we outline user profile settings that are available to profiles with Customer Community, Customer Community Plus, Partner Community, External Apps, or Channel Account licenses.

 **Note:** As a best practice, always clone the standard profile associated with a community license, and change object permissions as needed. If you want to limit the number of cloned profiles, use permission sets to assign object permissions.

License Name	External Apps License ²	Customer Community License	Customer Community Plus License	Partner Community License	Channel Account License
SKU Name	Commerce Portals SKU	Customer Community SKU	Customer Community Plus SKU	<ul style="list-style-type: none"> Partner Relationship Management (PRM) SKU External Apps SKU 	Channel Account SKU
Use Case	B2C	B2C	B2B	B2B	B2B
Salesforce Standard Objects					
Account Contact Relationships (Contacts to Multiple Accounts) ⁴	✓	✓	✓	✓	✓
Accounts	✓ Read, Edit	✓ Read, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit
Assets	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit
Campaigns				✓ Read, Create, and Edit ⁵	✓ Read, Create, and Edit ⁶
Cases		✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit

7

² The External Apps license can be purchased using a variety of SKUs, including the Commerce Portals SKU. After purchasing the Commerce Portals SKU, you see External Apps licenses in your org. A SKU includes licenses and additional functionality.

³ The Partner Community license can be purchased using a variety of SKUs, including the External Apps SKU. After purchasing the External Apps SKU, you see Partner Community licenses in your org. A SKU includes licenses and additional functionality.

⁴ To view or create relationships between accounts and contacts, you must have “Read” on accounts and contacts. To edit or delete relationships between account and contacts, you must have “Read” on accounts and “Edit” on contacts.

⁵ For the Partner Community license, to read, create, and edit campaigns in the user interface, the partner user also needs the “Marketing User” permission. With these permissions, a partner user can: search for and add their contacts or leads as campaign members, access reports on their campaigns, and mass-assign their contacts and leads on a campaign.

⁶ For the Channel Account license, to read, create, and edit campaigns in the user interface, the partner user also needs the “Marketing User” permission. With these permissions, a partner user can: search for and add their contacts or leads as campaign members, access reports on their campaigns, and mass-assign their contacts and leads on a campaign.

⁷ Customer Community Plus users can’t change the account or contact on a case they own. The owner of the case must be an internal or Partner Community user to make the change.

License Name	External Apps License	Customer Community License	Customer Community Plus License	Partner Community License	Channel Account License
SKU Name	Commerce Portals SKU	Customer Community SKU	Customer Community Plus SKU	<ul style="list-style-type: none"> Partner Relationship Management (PRM) SKU External Apps SKU 	Channel Account SKU
Use Case	B2C	B2C	B2B	B2B	B2B
Contacts	Read, Create, Edit	Read, Create, Edit	Read, Create, Edit	Read, Create, Edit	Read, Create, Edit
Contracts	Read, Create, Edit	Read, Create, Edit, Delete	Read, Create, Edit, Delete	Read, Create, Edit, Delete	Read, Create, Edit, Delete
Dashboards			Read Only		
Documents	Read Only	Read Only	Read Only	Read Only	Read Only
Entitlements		Read, Create, Edit	Read, Create, Edit	Read, Create, Edit	Read, Create, Edit
External Objects (Salesforce Connect)	Read, Create, Edit	Read, Create, Edit	Read, Create, Edit	Read, Create, Edit	Read, Create, Edit
Events and Calendar		Read ⁸	Read, Create, Edit, Delete ⁹	Read, Create, Edit, Delete	Read, Create, Edit, Delete
Ideas	Read, Create, Edit	Read, Create	Read, Create	Read, Create	Read, Create

² The External Apps license can be purchased using a variety of SKUs, including the Commerce Portals SKU. After purchasing the Commerce Portals SKU, you see External Apps licenses in your org. A SKU includes licenses and additional functionality.

³ The Partner Community license can be purchased using a variety of SKUs, including the External Apps SKU. After purchasing the External Apps SKU, you see Partner Community licenses in your org. A SKU includes licenses and additional functionality.

⁸ Customer Community license users can't add invitees to calendar events.

⁹ Customer Community Plus license users can't add invitees to calendar events.

License Name	External Apps License	Customer Community License	Customer Community Plus License	Partner Community License	Channel Account License
SKU Name	Commerce Portals SKU	Customer Community SKU	Customer Community Plus SKU	<ul style="list-style-type: none"> Partner Relationship Management (PRM) SKU External Apps SKU 	Channel Account SKU
Use Case	B2C	B2C	B2B	B2B	B2B
Leads				 Read, Create, Edit	 Read, Create, Edit
List Views	 Read, Create, Edit	 Read, Create, Edit	 Read, Create, Edit	 Read, Create, Edit	 Read, Create, Edit
Notes and Attachments		 Exceptions apply 10			
Opportunities				 Read, Create, Edit	 Read, Create, Edit
Orders	 Read, Create, Edit, Delete	 Read, Create, Edit, Delete	 Read, Create, Edit, Delete	 Read, Create, Edit, Delete	 Read, Create, Edit, Delete
Price Books	 Read Only	 Read Only	 Read Only	 Read Only	 Read Only
Products	 Read Only	 Read Only	 Read Only	 Read Only	 Read Only

² The External Apps license can be purchased using a variety of SKUs, including the Commerce Portals SKU. After purchasing the Commerce Portals SKU, you see External Apps licenses in your org. A SKU includes licenses and additional functionality.

³ The Partner Community license can be purchased using a variety of SKUs, including the External Apps SKU. After purchasing the External Apps SKU, you see Partner Community licenses in your org. A SKU includes licenses and additional functionality.

¹⁰ Only internal users can create notes and only in Salesforce Classic. Notes appear in the Notes & Attachment section of the record. After a note is created, both internal and Experience Cloud site users can access it. The site user's level of access on the note depends on their level of access on the record.

Both internal and Experience Cloud site users (with Customer Community, Customer Community Plus, and Partner Community licenses) can create Enhanced Notes using the New Note quick action on the record detail page in Experience Builder sites. Notes are available in the Notes related list. Enhanced Notes aren't available in sites created using Salesforce Tabs +Visualforce.

License Name	External Apps License	Customer Community License	Customer Community Plus License	Partner Community License	Channel Account License
SKU Name	Commerce Portals SKU	Customer Community SKU	Customer Community Plus SKU	<ul style="list-style-type: none"> Partner Relationship Management (PRM) SKU External Apps SKU 	Channel Account SKU
Use Case	B2C	B2C	B2B	B2B	B2B
Quotes				 Read, Create, Edit	 Read, Create, Edit
Reports ¹¹			 Create and Manage	 Create and Manage	 Create and Manage
Return Orders		 Read, Create, Edit	 Read, Create, Edit	 Read, Create, Edit	 Read, Create, Edit
Salesforce CMS Functionality ¹²					
Service Appointment		 Read, Create, Edit	 Read, Create, Edit	 Read, Create, Edit	 Read, Create, Edit
Task	Read Only	 Read, Create, Edit, Delete	 Read, Create, Edit, Delete	 Read, Create, Edit, Delete	 Read, Create, Edit, Delete
Work Order		 Read, Create, Edit	 Read, Create, Edit	 Read, Create, Edit	 Read, Create, Edit

² The External Apps license can be purchased using a variety of SKUs, including the Commerce Portals SKU. After purchasing the Commerce Portals SKU, you see External Apps licenses in your org. A SKU includes licenses and additional functionality.

³ The Partner Community license can be purchased using a variety of SKUs, including the External Apps SKU. After purchasing the External Apps SKU, you see Partner Community licenses in your org. A SKU includes licenses and additional functionality.

¹¹ To create and edit reports, the user also needs the “Create and Customize Reports,” “Report Builder,” and “Edit My Reports” permissions. For more information see, [Set Up Report Management for External Users—Create and Edit Reports](#). The Customer Community Plus license doesn't include support for report subscriptions.

¹² Functionality includes creating content types, previewing headless content in the site, scheduling headless content, and the Micosites LWR site template and its associated components.

¹³ Customer Community Users can't send email messages via Apex class when the parameter is set to setSaveAsActivity = true.

License Name	External Apps License ²	Customer Community License	Customer Community Plus License	Partner Community License	Channel Account License
SKU Name	Commerce Portals SKU	Customer Community SKU	Customer Community Plus SKU	<ul style="list-style-type: none"> Partner Relationship Management (PRM) SKU External Apps SKU 	Channel Account SKU
Use Case	B2C	B2C	B2B	B2B	B2B
Work Order Line Item		 Read, Create, Edit	 Read, Create, Edit	 Read, Create, Edit	 Read, Create, Edit
Salesforce Features, Capability, and Custom Objects					
Extra Data Storage	10 MB per user (member-based license)		2 MB per user (member-based license) 1 MB per user (login-based license)	When purchased with the PRM SKU: <ul style="list-style-type: none"> 5 MB per user (member-based license) 1 MB per user (login-based license) When purchased with the External Apps SKU: <ul style="list-style-type: none"> 45 MB per user (member-based license) 20 MB per login (login-based license) 	5 MB per user (member-based license) 1 MB per user (login-based license)
API Calls per Day (by Org)	<ul style="list-style-type: none"> 200 calls per day per user (member-based license) 	0	<ul style="list-style-type: none"> 200 calls per day per user (member-based license) 	When purchased with the PRM SKU: <ul style="list-style-type: none"> 200 calls per day per user 	<ul style="list-style-type: none"> 200 calls per day per user (member-based license)

² The External Apps license can be purchased using a variety of SKUs, including the Commerce Portals SKU. After purchasing the Commerce Portals SKU, you see External Apps licenses in your org. A SKU includes licenses and additional functionality.

³ The Partner Community license can be purchased using a variety of SKUs, including the External Apps SKU. After purchasing the External Apps SKU, you see Partner Community licenses in your org. A SKU includes licenses and additional functionality.

License Name	External Apps License ²	Customer Community License	Customer Community Plus License	Partner Community License	Channel Account License
SKU Name	Commerce Portals SKU	Customer Community SKU	Customer Community Plus SKU	<ul style="list-style-type: none"> Partner Relationship Management (PRM) SKU External Apps SKU 	Channel Account SKU
Use Case	B2C	B2C	B2B	B2B	B2B
	<ul style="list-style-type: none"> 400 calls per day per user (login-based license) 		<ul style="list-style-type: none"> 10 calls per day per user (login-based license) 	<ul style="list-style-type: none"> (member-based license) 10 calls per day per user (login-based license) <p>When purchased with the External Apps SKU:</p> <ul style="list-style-type: none"> 1000 calls per day per user (member-based license) 400 calls per day per user (login-based license) 	<ul style="list-style-type: none"> 10 calls per day per user (login-based license)
Chatter (People, Groups, Feeds, Private Messages)	✔	✔	✔	✔	✔
Custom Objects	✔	✔	✔	✔	✔
	100 custom objects per license (custom objects in managed packages don't count towards this	10 custom objects per license (custom objects in managed packages don't count towards this limit, as	10 custom objects per license (custom objects in managed packages don't count towards this limit, as long as	When purchased with the PRM SKU: 10 custom objects per license When purchased with the External	10 custom objects per license (custom objects in managed packages don't count towards this

² The External Apps license can be purchased using a variety of SKUs, including the Commerce Portals SKU. After purchasing the Commerce Portals SKU, you see External Apps licenses in your org. A SKU includes licenses and additional functionality.

³ The Partner Community license can be purchased using a variety of SKUs, including the External Apps SKU. After purchasing the External Apps SKU, you see Partner Community licenses in your org. A SKU includes licenses and additional functionality.

License Name	External Apps License	Customer Community License	Customer Community Plus License	Partner Community License	Channel Account License
SKU Name	Commerce Portals SKU	Customer Community SKU	Customer Community Plus SKU	<ul style="list-style-type: none"> Partner Relationship Management (PRM) SKU External Apps SKU 	Channel Account SKU
Use Case	B2C	B2C	B2B	B2B	B2B
	limit, as long as they're made publicly available on AppExchange)	long as they're made publicly available on AppExchange)	they're made publicly available on AppExchange)	Apps SKU: 100 custom objects per license Custom objects in managed packages don't count towards this limit, as long as they're made publicly available on AppExchange.	limit, as long as they're made publicly available on AppExchange))
Delegated Administration			✓	✓	✓
Einstein Lead Scoring and Einstein Opportunity Scoring ¹⁴				✓	✓
Enhanced List Views for Sales objects: Contact Intelligence View, Lead Intelligence View, and Pipeline Inspection ¹⁵				✓	✓

² The External Apps license can be purchased using a variety of SKUs, including the Commerce Portals SKU. After purchasing the Commerce Portals SKU, you see External Apps licenses in your org. A SKU includes licenses and additional functionality.

³ The Partner Community license can be purchased using a variety of SKUs, including the External Apps SKU. After purchasing the External Apps SKU, you see Partner Community licenses in your org. A SKU includes licenses and additional functionality.

¹⁴ See which editions support [Einstein Lead Scoring and Einstein Opportunity Scoring](#).

¹⁵ Some Enhanced List View features require Sales Cloud Einstein. See which editions support [Sales Cloud Einstein](#).

License Name	External Apps License	Customer Community License	Customer Community Plus License	Partner Community License	Channel Account License
SKU Name	Commerce Portals SKU	Customer Community SKU	Customer Community Plus SKU	<ul style="list-style-type: none"> Partner Relationship Management (PRM) SKU External Apps SKU 	Channel Account SKU
Use Case	B2C	B2C	B2B	B2B	B2B
Files ^{16,17}	 Content Libraries aren't available with External Apps licenses.	 Content Libraries aren't available with Customer Community licenses.	 Create, Read, Edit, Delete	 Create, Read, Edit, Delete	 Create, Read, Edit, Delete
Knowledge					
Market Development Funds					
Roles and Standard Sharing					
Sharing Sets ¹⁸					
Salesforce App					
Send Email				 ¹⁹	 ²⁰
Territory Management					
Recognition Badges ²¹					

² The External Apps license can be purchased using a variety of SKUs, including the Commerce Portals SKU. After purchasing the Commerce Portals SKU, you see External Apps licenses in your org. A SKU includes licenses and additional functionality.

³ The Partner Community license can be purchased using a variety of SKUs, including the External Apps SKU. After purchasing the External Apps SKU, you see Partner Community licenses in your org. A SKU includes licenses and additional functionality.

¹⁶ Salesforce Files with Chatter enabled lets you share files in a group, feed, and post a file to a record. With Salesforce CRM Content enabled, Files gives you access to Libraries, content deliveries, and file tagging.

¹⁷ Library administrators can manage library permissions to determine the level of access users have to content libraries.

¹⁸ Sharing sets aren't supported by reports and dashboards. Permission sets can be used in tandem with sharing sets to allow customers to access reports and dashboards.

¹⁹ Partner users can't see emails in the case feed.

²⁰ Channel Account users can't see emails in the case feed.

²¹ Recognition Badges is only available in Lightning Communities.

License Name	External Apps License	Customer Community License	Customer Community Plus License	Partner Community License	Channel Account License
SKU Name	Commerce Portals SKU	Customer Community SKU	Customer Community Plus SKU	<ul style="list-style-type: none"> Partner Relationship Management (PRM) SKU External Apps SKU 	Channel Account SKU
Use Case	B2C	B2C	B2B	B2B	B2B
Workflow Approvals		✓ ²²	✓	✓	✓

 **Note:** Starting with Summer '13, the Customer Portal user license isn't available for new orgs. You can create a customer portal using the Customer Account Portal Lightning template in Experience Builder.

Existing orgs using Customer Portal licenses may continue to use their licenses.

If you're still working with the Customer Portal, see the [Customer Portal Guide](#) for more information.

SEE ALSO:

[User Licenses](#)

[When to Use an Internal or External License](#)

[Upgrade Experience Cloud User Licenses](#)

[Create Experience Cloud Site Users](#)

[Authenticated Website User Licenses](#)

[Partner Portal User Licenses](#)

[Customer Portal User Licenses](#)

[Lightning Platform Starter and Lightning Platform Plus Details](#)

² The External Apps license can be purchased using a variety of SKUs, including the Commerce Portals SKU. After purchasing the Commerce Portals SKU, you see External Apps licenses in your org. A SKU includes licenses and additional functionality.

³ The Partner Community license can be purchased using a variety of SKUs, including the External Apps SKU. After purchasing the External Apps SKU, you see Partner Community licenses in your org. A SKU includes licenses and additional functionality.

²² Customer Community license holders can submit for approval and can be assigned as the approver, but they can't be assigned tasks or email alerts via approval workflows.

Channel Account Licenses

The Channel Account license is available for Experience Cloud sites and has the same permission and feature access as the Partner Community license. Unlike login or member-based licenses, Channel Account licenses are priced per partner account. Partners then open up access to users.

 **Important:** Experience Cloud sites use community user licenses.

Community License Name	Best Used For	Comparable Portal License
Channel Account	Business-to-business sites and portals that calculate their usage based on number of partners instead of number of individual users.	Partner

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

Learn About the License

What are partner-based licenses?

A partner-based license is considered an external license, and gives you the power to buy a specific number of licenses for your partner accounts. Each partner account with an assigned license is given up to 40 partner users. User licenses are pooled, making it less likely for individual partners to exceed their user limits. Extra users, beyond the typical 40, can be purchased if necessary.

For example, if you have five franchisee partner accounts, 10 system integrator partner accounts, and 15 broker partner accounts, you'd purchase 30 Channel Account licenses. Each account could add up to 40 users, for a total of 1200 potential partner users accessing your partner site.

When do you use a partner-based license?

Use the Channel Account license when you want to give your partner users access to Experience Cloud sites, but aren't sure how many users need access. By purchasing the number of licenses you need for partner accounts, you can give your partners the power to manage their own users.

 **Note:** The Channel Account license offers the same permission structure as the Partner license. For more information, see [Experience Cloud User Licenses](#).

Lightning Platform Starter and Lightning Platform Plus Details

Lightning Platform Starter and Lightning Platform Plus both contain a Salesforce Platform license and a Company Communities Permission Set License. This table shows which features are available to users granted a Salesforce Platform license and assigned the Company Communities Permission Set License.

Details

	Lightning Platform Starter	Lightning Platform Plus
Salesforce Standard Objects		

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

	Lightning Platform Starter	Lightning Platform Plus
Account Contact Relationships (Contacts to Multiple Accounts) ²³	✓	✓
Accounts	✓ Read, Create, Edit, Delete, View All Data, Manage All Data	✓ Read, Create, Edit, Delete, View All Data, Manage All Data
Assets	✓ Read, Create, Edit, Delete	✓ Read, Create, Edit, Delete
Campaigns		
Cases	✓ Read, Create, Edit, Delete ²⁴	✓ Read, Create, Edit, Delete ²⁵
Contacts	✓ Read, Create, Edit, Delete, View All Data, Manage All Data	✓ Read, Create, Edit, Delete, View All Data, Manage All Data
Contracts		
Dashboards	✓	✓
Documents	✓ Read, Create, Edit, Delete, View All Data, Manage All Data	✓ Read, Create, Edit, Delete, View All Data, Manage All Data
Entitlements		
External Objects (Salesforce Connect)	✓ Read, Create, Edit	✓ Read, Create, Edit
Events and Calendar	✓ Read, Create, Edit, Delete	✓ Read, Create, Edit, Delete
Ideas	✓ Read, Create	✓ Read, Create
Leads		
List Email	✓	✓

²³ To view or create relationships between accounts and contacts, you must have “Read” on accounts and contacts. To edit or delete relationships between account and contacts, you must have “Read” on accounts and “Edit” on contacts.

²⁴ For Lightning Platform Starter licenses, using cases for customer service purposes, even internally, requires a Service Cloud license.

²⁵ For Lightning Platform Plus licenses, using cases for customer service purposes, even internally, requires a Service Cloud license.

	Lightning Platform Starter	Lightning Platform Plus
List Views	 Read, Create, Edit, Delete	 Read, Create, Edit, Delete
Notes and Attachments		
Opportunities		
Orders		
Price Books		
Products		
Quotes		
Reports ²⁶	 Read, Create, Edit, Delete	 Read, Create, Edit, Delete
Service Appointment		
Task	 Read, Create, Edit, Delete	 Read, Create, Edit, Delete
Work Order	 Read, Create, Edit, Delete (Can be used for employees, but not external users (e.g. customers, partners))	 Read, Create, Edit, Delete (Can be used for employees, but not external users (e.g. customers, partners))
Work Order Line Item	 Read, Create, Edit, Delete	 Read, Create, Edit, Delete
Salesforce Features, Capability, and Custom Objects		
Additional Data Storage	20 MB per user (user-based license) ²⁷	20 MB per user (user-based license) ²⁸
API Calls per Day (by Org)	200 per member for Enterprise Edition or Unlimited Edition orgs	1000 per member for Enterprise Edition orgs 5000 per member for Unlimited Edition orgs
Chatter (People, Groups, Feeds, Private Messages)		

²⁶ To create and edit reports, the user also needs the “Create and Customize Reports,” “Report Builder,” and “Edit My Reports” permissions. For more information see, [Set Up Report Management for External Users—Create and Edit Reports](#). Report creation is available only in Salesforce Tabs + Visualforce communities.

²⁷ For the Lightning Platform Starter license, the data storage limit is 20 MB per user license, and the file storage limit is 2 GB per user license.

²⁸ For the Lightning Platform Plus license, the data storage limit is 20 MB per user license for EE editions, and 120 MB per user license for UE editions. File storage limit is 2 GB per user license.

	Lightning Platform Starter	Lightning Platform Plus
Custom Objects	 10 custom objects per license (custom objects in managed packages don't count towards this limit, as long as they are made publicly available on AppExchange))	 110 custom objects per license (custom objects in managed packages don't count towards this limit, as long as they are made publicly available on AppExchange))
Delegated Administration		
Files ²⁹ and Content ³⁰	 Create, Read, Edit, Delete	 Create, Read, Edit, Delete
Knowledge	 Read Only	 Read Only
Roles and Advanced Sharing	 	
Sharing Sets ³¹		
Salesforce App	 	
Send Email	 	
Territory Management		
Recognition Badges ³²	 	
Tokens	 Create, Read, Edit, Delete	 Create, Read, Edit, Delete
Workflow Approvals	 	

 **Note:** Assign Lightning Platform Starter and Lightning Platform Plus users a profile or permission set that allows access only to the allowed objects and the number of custom objects indicated in the table.

Lightning Platform Starter and Lightning Platform Plus users must be internal employees or contractors. These users can't complete internal or external customer service work without a Service Cloud license.

SEE ALSO:

[Experience Cloud User Licenses](#)

²⁹ Salesforce Files with Chatter enabled lets you share files in a group, feed, and post a file to a record. With Salesforce CRM Content enabled, Files gives you access to Libraries, content deliveries, and file tagging.

³⁰ Library administrators can manage library permissions to determine the level of access users have to content libraries.

³¹ Sharing sets are not supported by reports and dashboards. Permission sets can be used in tandem with sharing sets to allow customers to access reports and dashboards.

³² Recognition Badges is only available in Lightning Communities.

Database.com User Licenses

User licenses designed for users who need to administer Database.com and who need Database.com access to data stored in Database.com.

User License	Description	Default Number of Available Licenses
Database.com Admin	Designed for users who need to administer Database.com, or make changes to Database.com schemas or other metadata using the point-and-click tools in the Database.com Console.	Database.com Edition: 3
Database.com User	Designed for users who need Database.com access to data stored in Database.com.	Database.com Edition: 3 Enterprise, Unlimited, and Database.com Edition: 0 Contact Database.com to obtain Database.com User Licenses
Database.com Light User	Designed for users who need only Database.com access to data, need to belong to Database.com groups (but no other groups), and don't need to belong to roles or queues. Access to data is determined by organization-wide sharing defaults.	Database.com Edition: 0 Enterprise, Unlimited, and Database.com Edition: 0 Contact Database.com to obtain Database.com Light User Licenses

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Database.com** Edition

SEE ALSO:

[User Licenses](#)

Service Cloud Portal User Licenses

Service Cloud Portal users have the High Volume Customer Portal license. This license gives contacts unlimited logins to your Service Cloud Portal to access customer support information.

Users with this license can access accounts, assets, cases, contacts, custom objects, documents, ideas, and questions, depending on their permission settings.

The Overage High Volume Customer Portal license is the same as the High Volume Customer Portal license, except that users do not have unlimited logins. Contact Salesforce for information about the number of Customer Portal licenses you can activate.

This table lists the permissions that can be assigned to Service Cloud portal users.

	Create	Read	Update	Delete
Accounts		✓	✓	
Assets	✓	✓	✓	
Cases	✓	✓	✓	
Contacts	✓	✓	✓	
Custom Objects	✓	✓	✓	✓
Documents		✓		
Ideas	✓	✓		
Knowledge		✓		
Price Books		✓		
Products		✓		
Questions and Answers	✓	✓		
Solutions		✓		
Work Orders	✓	✓	✓	

SEE ALSO:

[User Licenses](#)

Sites and Site.com User Licenses

Sites and Site.com users can have Guest User or Site.com Only user licenses.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Edition requirements vary by user license type.

Guest User Designed for public users who access your Site.com or Experience Cloud sites. If digital experiences are enabled, these users also have access to public pages in your Experience Cloud sites. Site visitors have access to any information made available in an active public site. Each site has a dedicated guest user profile.

For Site.com, **Developer, Enterprise, Unlimited,** and **Performance** Editions each come with unlimited Guest User licenses.

For Salesforce sites, **Enterprise, Unlimited,** and **Performance** Editions come with 100 Guest User licenses. **Developer** Edition comes with one Guest User license.

- You can't purchase additional Guest User licenses for Salesforce sites.
- The Authenticated Website high-volume portal user license is specifically designed to be used with Salesforce sites. Because it's designed for high volumes, it should be a cost-effective option to use with Salesforce sites.

Site.com Only Designed for **Performance, Unlimited,** and **Enterprise** Edition users who need access to Site.com but not to standard CRM functionality. Site.com Only users are entitled to the same rights as Lightning Platform - One App users, plus they have access to the Content app. However, they don't have access to the Accounts and Contacts objects. Users have access to an unlimited number of custom tabs but are limited to the use of one custom app, which is defined as up to 20 custom objects.

Each Site.com Only user also needs either a Site.com Contributor or Site.com Publisher feature license to access Site.com.

SEE ALSO:

[User Licenses](#)

Authenticated Website User Licenses

Platform portal users have the Authenticated Website license, which is designed to be used with Salesforce Sites. It gives named sites users unlimited logins to your Platform Portal to access customer support information.

The Overage Authenticated Website license is the same as the Authenticated Website license, except that users do not have unlimited logins.

 **Note:** When orders are enabled, standard profiles automatically include all object permissions for orders, as well as read access for products and price books. If your external users are assigned to a standard profile and these object permissions aren't appropriate for them, consider creating custom profiles that don't include these object permissions.

This table lists the permissions that can be given to Authenticated Website users.

	Create	Read	Update	Delete
Contracts	✓	✓	✓	✓
Documents		✓		
Ideas	✓	✓		
Knowledge		✓		
Orders	✓	✓	✓	✓

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

	Create	Read	Update	Delete
Price Books		✓		
Products		✓		
Custom Objects	✓	✓	✓	✓

SEE ALSO:

[User Licenses](#)

Legacy Portal Licenses

The following licenses are used in portals: Gold Partner, Customer Portal Manager Standard, and Customer Portal Manager Custom. These licenses are no longer sold because Partner Portals and Customer Portals are no longer available for orgs that aren't currently using them. Instead, use Experience Cloud sites.

 **Note:** Starting with Summer '13, these licenses are only available for organizations that already have a Partner Portal or Customer Portal. If you don't have a Partner Portal or Customer Portal but want to easily share information with your partners or customers, see [Experience Cloud User Licenses](#).

Partner Portal User Licenses

Partner Portal users have the Gold Partner user license. They can only access Salesforce using the partner portal.

 **Note:** When orders are enabled, standard profiles automatically include all object permissions for orders, as well as read access for products and price books. If your external users are assigned to a standard profile and these object permissions aren't appropriate for them, consider creating custom profiles that don't include these object permissions.

Take a look at this table, which shows the equivalent current communities licenses for legacy portal licenses.

 **Important:** Experience Cloud sites use community user licenses.

License Name	Best Used For	Comparable Portal License
External Apps	Custom digital experiences to engage any external stakeholder, including Brand Engagement and Customer Loyalty. Limited access to CRM objects. The External Apps license can be used with person accounts.	High Volume Customer Portal, Service Cloud Portal, Authenticated Sites Portal
Customer Community	Business-to-consumer experiences with large numbers of external users who need access to case objects or knowledge. The Customer Community can be used with person accounts.	High Volume Customer Portal, Service Cloud Portal, Authenticated Sites Portal

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

License Name	Best Used For	Comparable Portal License
Customer Community Plus	Business-to-consumer experiences with external users who need access to reports and dashboards and need standard sharing . The Customer Community Plus can be used with person accounts.	Customer Portal — Enterprise Administration, Customer Portal Manager Standard, Customer Portal Manager Custom
Partner Community	Business-to-business experiences that need access to sales data such as partner relationship management. The Partner Community can't be used with person accounts.	Gold Partner
Channel Account	Business-to-business sites and portals that calculate their usage based on number of partners instead of number of individual users.	Gold Partner

Refer to the permissions table found in the [Experience Cloud User Licenses](#) to see the permissions allowed by your equivalent license.

Customer Portal User Licenses

Users of a Customer Portal site have the Customer Portal Manager Standard license.

It allows contacts to log in to your Customer Portal to manage customer support. You can associate users who have a Customer Portal Manager Standard license with the Customer Portal User profile or a profile cloned and customized from the Customer Portal User profile. This standard profile lets users view and edit data they directly own or data owned by or shared with users below them in the Customer Portal role hierarchy. These users can also view and edit cases where they're listed in the `Contact Name` field.

Users with the Customer Portal Manager Standard license can:

- View contacts, price books, and products.
- View and edit accounts and cases.
- Create and edit assets.
- Create, view, edit, and delete custom objects.
- Access custom objects depending on their permissions.
- Receive the "Portal Super User" permission.
- Access Salesforce CRM Content if they have a Salesforce CRM Content feature license or the appropriate permissions.

The Overage Customer Portal Manager Standard license is the same as the Customer Portal Manager Standard license, except that users are limited to one login per month.

 **Note:** When orders are enabled, standard profiles automatically include all object permissions for orders, as well as read access for products and price books. If your external users are assigned to a standard profile and these object permissions aren't appropriate for them, consider creating custom profiles that don't include these object permissions.

Take a look at this table, which shows the equivalent current communities licenses for legacy portal licenses.

 **Important:** Experience Cloud sites use community user licenses.

EDITIONS

Available in: **Salesforce Classic** ([not available in all orgs](#))

Available in: **Enterprise, Performance, Unlimited, and Developer** Editions

License Name	Best Used For	Comparable Portal License
External Apps	Custom digital experiences to engage any external stakeholder, including Brand Engagement and Customer Loyalty. Limited access to CRM objects. The External Apps license can be used with person accounts.	High Volume Customer Portal, Service Cloud Portal, Authenticated Sites Portal
Customer Community	Business-to-consumer experiences with large numbers of external users who need access to case objects or knowledge. The Customer Community can be used with person accounts.	High Volume Customer Portal, Service Cloud Portal, Authenticated Sites Portal
Customer Community Plus	Business-to-consumer experiences with external users who need access to reports and dashboards and need standard sharing . The Customer Community Plus can be used with person accounts.	Customer Portal — Enterprise Administration, Customer Portal Manager Standard, Customer Portal Manager Custom
Partner Community	Business-to-business experiences that need access to sales data such as partner relationship management. The Partner Community can't be used with person accounts.	Gold Partner
Channel Account	Business-to-business sites and portals that calculate their usage based on number of partners instead of number of individual users.	Gold Partner

Refer to the permissions table found in the [Experience Cloud User Licenses](#) to see the permissions allowed by your equivalent license.

Customer Portal—Enterprise Administration User Licenses

Customer Portal—Enterprise Administration users have the Customer Portal Manager Custom license. This license gives contacts unlimited logins to your Salesforce Customer Portal to manage customer support.

You can associate users who have a Customer Portal Manager Custom license with the Customer Portal User profile or a profile cloned and customized from the Customer Portal User profile, which lets them view and edit data they directly own and view, create, and edit cases where they're listed in the `Contact` Name field.

Users with this license can:

- Create, read, or update accounts, assets, and cases.
- View contacts.
- View custom objects and run reports depending on their permissions.
- Receive the "Portal Super User" and "Delegated External User Administrator" permissions.
- Access Salesforce CRM Content if they have a Salesforce CRM Content feature license or the appropriate permissions.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Enterprise, Performance, Unlimited, and Developer** editions

The Overage Customer Portal Manager Custom license is the same as the Customer Portal Manager Custom license, except that users don't have unlimited logins. Contact Salesforce for information about the number of Customer Portal licenses you can activate.

 **Note:** Once orders are enabled, standard profiles automatically include all object permissions for orders, as well as read access for products and price books. If your external users are assigned to a standard profile and these object permissions aren't appropriate for them, consider creating custom profiles that don't include these object permissions.

Take a look at this table, which shows the equivalent current communities licenses for legacy portal licenses.

 **Important:** Experience Cloud sites use community user licenses.

License Name	Best Used For	Comparable Portal License
External Apps	Custom digital experiences to engage any external stakeholder, including Brand Engagement and Customer Loyalty. Limited access to CRM objects. The External Apps license can be used with person accounts.	High Volume Customer Portal, Service Cloud Portal, Authenticated Sites Portal
Customer Community	Business-to-consumer experiences with large numbers of external users who need access to case objects or knowledge. The Customer Community can be used with person accounts.	High Volume Customer Portal, Service Cloud Portal, Authenticated Sites Portal
Customer Community Plus	Business-to-consumer experiences with external users who need access to reports and dashboards and need standard sharing . The Customer Community Plus can be used with person accounts.	Customer Portal — Enterprise Administration, Customer Portal Manager Standard, Customer Portal Manager Custom
Partner Community	Business-to-business experiences that need access to sales data such as partner relationship management. The Partner Community can't be used with person accounts.	Gold Partner
Channel Account	Business-to-business sites and portals that calculate their usage based on number of partners instead of number of individual users.	Gold Partner

Refer to the permissions table found in the [Experience Cloud User Licenses](#) to see the permissions allowed by your equivalent license.

Permission Set Licenses

Permission set licenses entitle users to access additional features not included in their assigned user license. Users can be assigned any number of permission set licenses.

For example, you previously assigned a user a Salesforce Platform user license, which entitled the user to the objects and functionality required for the user's day-to-day tasks. You now want this user to have access to Lightning console apps, which isn't included in their user license. You purchase and assign a Lightning Console permission set license to the user, which allows them to be granted the Lightning Console User permission. After you grant this user this permission via a permission set, the user can use Lightning Console apps.

Permission set licenses and permission sets have different purposes.

- **Permission set licenses** extend the functionality of user licenses. With permission set licenses, you can assign more permissions to users than their user license supports.
- **Permission sets** extend users' functional access without changing their profiles.

Said another way, users' assigned licenses define the maximum functionality available to them. Admins use permission sets to control the subset of permissions that each user has, so that each license can be tailored to fit numerous different user roles. For users to access additional license functionality, they must both be assigned the permission set license and a permission set containing the feature permissions. If you assign users permissions via a permission set and they don't have the required licenses, you receive an assignment error.

Some permission set licenses come with auto-generated standard permission sets, which make the administration process easier. When you assign users the standard permission set, these users are automatically assigned the related permission set license. For info on specific permission set licenses, see the related feature documentation.

[View and Manage Your Permission Set Licenses](#)

View information about the permission set licenses that you purchased and manage user assignments.

[Create a Permission Set Associated with a Permission Set License](#)

For users to access license functionality, they must both be assigned the permission set license and a permission set containing the feature permissions.

[Assign a Permission Set License to a User](#)

You might need to assign a permission set license to a user before you can assign certain permissions.

[Remove a Permission Set License from a User](#)

First remove or modify the relevant assigned permission sets that require the license, and then remove the assigned permission set license.

SEE ALSO:

[Permission Sets](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

The availability of each permission set license depends on the edition requirements for permission sets and the related feature.

View and Manage Your Permission Set Licenses

View information about the permission set licenses that you purchased and manage user assignments.

To learn how to check your remaining licenses, watch [How Many Licenses Have I Used? \(English Only\)](#).

1. From Setup, in the Quick Find box, enter *Company Information*, and then select **Company Information**.
2. View the Permission Set Licenses related list.
3. Click the name of the permission set license to see more details. On this page, you can see information on available seats and the permissions included in the license.

EDITIONS

Available in: both Salesforce Classic (**not available in all orgs**) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To view permission set licenses:

- [View Setup and Configuration](#)

Permission Set License IdentityConnect [View Users](#) [Assign Users](#) [Enable for Integrations](#)

View information about this permission set license and manage assignments. Permission set licenses extend the functionality of user licenses. You can enable this permission set license for integrations to allow Salesforce integration features to access the necessary data. If integrations are required for feature functionality and the license isn't enabled for integrations, you receive an error when setting up the session-based permission set or executing the feature.

Properties	
Name	IdentityConnect
Label	Identity Connect
Enabled for Integrations	false

Expiration	
Status	Active

Seats	
Total Licensed Seats	10
Total Used Seats	1
Available Seats	9

Permissions	
User Permissions	• Use Identity Connect
Object Permissions	
Custom Permissions	

[View Users](#) [Assign Users](#) [Enable for Integrations](#)

4. To view users already assigned to this permission set license, click **View Users**.
5. To assign users to the license, click **Assign Users**. You can assign multiple users at the same time.
6. Optionally, to enable this permission set license for integrations and allow Salesforce integration features to access data, click **Enable for Integrations**.

Note: If integrations are required for feature functionality and the license isn't enabled for integrations, you receive an error when setting up the session-based permission set or executing the feature. Only enable integrations if necessary for the feature.

For information on purchasing permission set licenses, contact your Salesforce account representative.

SEE ALSO:

[Permission Set Licenses](#)

[Assign a Permission Set License to a User](#)

Create a Permission Set Associated with a Permission Set License

For users to access license functionality, they must both be assigned the permission set license and a permission set containing the feature permissions.

Make sure to follow instructions for your permission set license-related feature. You can't add permission sets that are associated with permission set licenses to managed packages. If you purchased a license that comes with standard permission sets, such as Sales User, permission sets are auto-generated for you.

1. From Setup, enter *Company Information* in the Quick Find box, then select **Company Information** and scroll down to Permission Set Licenses.
2. From Setup, enter *Permission Sets* in the Quick Find box, then select **Permission Sets**.
3. Click **New**.
4. Enter your permission set information.
5. For License, select the license to associate with this permission set.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer Editions**

USER PERMISSIONS

To assign a permission set license:

- Manage Users

To assign a permission set to users:

- Assign Permission Sets

Save Cancel

Enter permission set information

Label

API Name ⓘ

Description

Select the type of users who will use this permission set

Who will use this permission set?

-Choose '--None--' if you plan to assign this permission set to multiple users with different user and permission set licenses.
 -Choose a specific user license if you want users with only one license type to use this permission set.
 -Choose a specific permission set license if you want this permission set license auto-assigned with the permission set.

Not sure what a permission set license is? [Learn more here.](#)

License ▼

Save Cancel

When you select a specific permission set license, any user assigned to the permission set is auto-assigned the permission set license. If you select --None--, you must manually assign the permission set license to users before you can add them to the new permission set.

6. Select the feature permissions to enable for your permission set. Use **Find Settings** to search for them quickly. Refer to the documentation for your feature to see which permissions are available with a specific permission set license.
-  **Example:** Let's say you purchased an Identity Connect permission set license. This permission set license contains a permission that grants access to the Identity Connect product features, such as providing Active Directory integration. To grant a user access to this permission:
- Ensure that the user has the Identity Connect permission set license. Users who don't have the associated permission set license for a permission set you create can't use the permission set. You can check which permission set licenses a user has by viewing the Permission Set License Assignments section of the user detail page.
 - Create a permission set and name it something like "Identity Connect Permissions." From License, choose **Identity Connect**. While still in the permission set, go to **Find Settings**, search for **Identity Connect**, and select the **Use Identity Connect** system permission.
 - Assign a user to the permission set.

SEE ALSO:

[Permission Set Licenses](#)
[Permission Sets](#)

Assign a Permission Set License to a User

You might need to assign a permission set license to a user before you can assign certain permissions.

 **Tip:** Before beginning, check if the permission set license is already associated with a permission set. If so, save yourself time and simply assign the user to that permission set. Follow the instructions for the specific permission set license you have.

1. To assign a permission set license to one user:
 - a. From Setup, enter *Users* in the Quick Find box, then select **Users**.
 - b. Click the name of the user to whom you want to assign the permission set license.
 - c. In the Permission Set License Assignments related list, click **Edit Assignments**.
 - d. Select the permission set license to assign.
2. To assign a permission set license to multiple users:
 - a. From Setup, in the Quick Find box, enter *Company Information*, and then select **Company Information**. Scroll down to the Permission Set Licenses section.
 - b. Click the name of the permission set license that you want to assign users to.
 - c. On the permission set license's detail page, click **Assign Users**.
 - d. Select the users that you want to assign, then click **Assign**.

Add the related permission to a permission set and then assign that permission set to the user.

SEE ALSO:

[Permission Set Licenses](#)

[Remove a Permission Set License from a User](#)

[Permission Sets](#)

[Manage Permission Set Assignments](#)

Remove a Permission Set License from a User

First remove or modify the relevant assigned permission sets that require the license, and then remove the assigned permission set license.

1. Identify the permission that requires the permission set license that you want to remove.
2. Make sure that permission isn't assigned to the user through a permission set. You can do that in one of these ways.
 - Remove the permission from the permission sets assigned to the user
 - [Remove the permission set](#) from the user's assigned permission sets
3. To remove a permission set license from a single user:
 - a. From Setup, in the Quick Find box, enter *Users*, and then select **Users**.
 - b. Click the name of the user whose permission set license you want to remove.
 - c. In the Permission Set License Assignments related list, click **Del** next to the permission set license that you want to remove, and then click **OK**.
4. To remove a permission set license from multiple users:

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To assign a permission set license:

- [Manage Users](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To remove a permission set license:

- [Manage Users](#)

- a. From Setup, in the Quick Find box, enter *Company Information*, and then select **Company Information**. Scroll down to the Permission Set Licenses section.
- b. Click the name of the permission set license you want to remove.
- c. On the permission set license's detail page, click **View Users**.
- d. Select the users that you want to remove assignments for. Click **Remove Assignments** and then click **OK**.

SEE ALSO:

[Permission Set Licenses](#)[View and Manage Your Permission Set Licenses](#)[Assign a Permission Set License to a User](#)

Feature Licenses Overview

A feature license entitles a user to access an additional feature that isn't included with his or her user license, such as Marketing or WDC. Users can be assigned any number of feature licenses.

Depending on the features that are enabled for your organization, you might be able to assign more than one type of feature license to your users. To purchase feature licenses, contact your Salesforce account representative.

[View Your Organization's Feature Licenses](#)

View the feature licenses your company has purchased to know what you have available to assign to your users.

[Enable a Feature License for a User](#)

You can enable a feature for a user in your organization when creating or editing that user.

[Available Feature Licenses](#)

Assign one or more of these additional feature licenses to users so that they can access features not included in their user license.

SEE ALSO:

[View and Manage Users](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Edition requirements vary for each feature license.

View Your Organization's Feature Licenses

View the feature licenses your company has purchased to know what you have available to assign to your users.

To learn how to check your remaining licenses, watch [▶ How Many Licenses Have I Used? \(English Only\)](#).

1. From Setup, enter *Company Information* in the **Quick Find** box, then select **Company Information**.
2. See the Feature Licenses related list.

For information on purchasing feature licenses, contact your Salesforce account representative.

SEE ALSO:

- [Feature Licenses Overview](#)
- [Available Feature Licenses](#)
- [Enable a Feature License for a User](#)
- [View and Manage Users](#)

Enable a Feature License for a User

You can enable a feature for a user in your organization when creating or editing that user.

1. In Setup, enter *Users* in the **Quick Find** box, then select **Users**.
2. In the user list view, click a user's name.
3. On the User Detail page, select the checkbox next to the feature license you want to enable for that user.
You can enable more than one feature license for a single user.
4. Click **Save**.

SEE ALSO:

- [Edit Users](#)
- [Add a Single User](#)
- [Feature Licenses Overview](#)
- [Available Feature Licenses](#)
- [View Your Organization's Feature Licenses](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To view feature licenses:

- View Setup and Configuration

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To enable feature licenses:

- Manage Internal Users

Available Feature Licenses

Assign one or more of these additional feature licenses to users so that they can access features not included in their user license.

Feature License	Enables a User to
Chatter Answers User	Access Chatter Answers. This feature license is automatically assigned to high-volume portal users who self-register for Chatter Answers.
Flow User	Run flows.
Knowledge User	Access Salesforce Knowledge.
Chat User	Access to Chat.
Marketing User	Create, edit, and delete campaigns, configure advanced campaign setup, and add campaign members and update their statuses with the Data Import Wizard.
Offline User	Access Connect Offline.
Salesforce CRM Content User	Access Salesforce CRM Content.
Service Cloud User	Access the Salesforce Console for Service.  Note: Access to the Salesforce Console for Sales requires the Sales Console User permission set license.
Site.com Contributor User	Edit site content on Site.com Studio.
Site.com Publisher User	Create and style websites, control the layout and functionality of pages and page elements, and add and edit content on Site.com Studio.
WDC User	Access to WDC objects and permissions.

For information on purchasing feature licenses, contact your Salesforce account representative.

SEE ALSO:

- [View Your Organization's Feature Licenses](#)
- [Enable a Feature License for a User](#)
- [View and Manage Users](#)
- [Feature Licenses Overview](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Usage-Based Entitlements

A usage-based entitlement is a limited resource that your organization can use on a periodic basis. For example, the allowed number of monthly logins to a Partner Community or the record limit for Data.com list users are usage-based entitlements.

Some entitlements are persistent. These entitlements give your Salesforce org a set number of the resource, and the amount allowed doesn't change unless your contract changes. For example, if your company purchases monthly subscriptions for 50 members to access a Partner Community, you can assign up to 50 individuals the ability to log into the community as many times as they want.

Other entitlements are not persistent; these entitlements work like credit. Your org can use up to the amount allowed of that entitlement over the time indicated by the resource's frequency. If the entitlement has a frequency of Once, your org must purchase more of the resource to replenish the allowance. If the entitlement has a frequency of Monthly, then your contract (not the calendar month) determines the start and end of the month.

For example:

- Company A purchases 50 monthly logins for a Partner Community, and on January 15 that org has a pool of 50 logins. Each time someone logs in, one login is used. On February 15, no matter how many were used in the previous month, the pool is refreshed and 50 logins are available through March 14.
- Company B purchases 2,000 records for Data.com list users with an end date of May 15. That org's list users can add or export up to 2,000 records until that date. If the org reaches that limit before May 15, the Data.com list users won't be able to add or export more records. To unblock users, Company B can purchase more records.

 **Note:** If your org has multiple contracts with the same `Resource` and the `Resource ID` is `(tenant)`, you still only see one row for that entitlement, but the data in that row reflects your combined contracts. In this case, `Start Date` reflects the earliest start date among those contracts, and `End Date` reflects the latest end date among those contracts. Like feature licenses, usage-based entitlements don't limit what you can do in Salesforce; they add to your functionality. If your usage exceeds the allowance, Salesforce will contact you to discuss additions to your contract.

[View Your Salesforce Org's Usage-Based Entitlements](#)

Look at your company's usage-based entitlements to know which resources your org is entitled to.

[Usage-Based Entitlement Fields](#)

The Usage-Based Entitlements related list displays the following information. These fields aren't editable, and they're only visible if your Salesforce org is entitled to a resource.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, and Professional with API Access** Editions

View Your Salesforce Org's Usage-Based Entitlements

Look at your company's usage-based entitlements to know which resources your org is entitled to.

To learn how to check your usage-based entitlements, watch [How Many Licenses Have I Used? \(English Only\)](#).

1. From Setup, enter *Company Information* in the **Quick Find** box, then select **Company Information**.
2. At the bottom of the Company Information page, view the Usage-Based Entitlements related list.

For information on purchasing usage-based entitlements, contact your Salesforce account representative.

SEE ALSO:

[Usage-Based Entitlements](#)

[Usage-Based Entitlement Fields](#)

Usage-Based Entitlement Fields

The Usage-Based Entitlements related list displays the following information. These fields aren't editable, and they're only visible if your Salesforce org is entitled to a resource.

Column name	Description
Resource	What your company can use.
Resource ID	Unique identifier for this line item.
Start Date	Day your contract begins.  Note: If you have multiple contracts affecting this resource, this field reflects the earliest start date among your contracts.
End Date	Day your contract ends.  Note: If you have multiple contracts affecting this resource, this field reflects the latest end date among your contracts.
Frequency	If Monthly, Allowance is reset at the beginning of each month. If Once, Allowance is available until End Date .

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

USER PERMISSIONS

To view usage-based entitlements:

- View Setup and Configuration

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

Column name	Description
Allowance	Amount of a resource that your org can use. If <code>Frequency</code> is <code>Monthly</code> , the month begins on your <code>Start Date</code> .
Amount Used	The amount of this resource that your org is using. This field is updated only on active production orgs. Sandbox and trial orgs aren't updated.
Last Updated	The most recent date and time when Salesforce took a snapshot of your org's usage for this resource. This field is updated only on active production orgs. Sandbox and trial orgs aren't updated.

For more information about resources your org is entitled to, contact your Salesforce account representative.

SEE ALSO:

[Usage-Based Entitlements](#)

[View Your Salesforce Org's Usage-Based Entitlements](#)

Delegate Administrative Duties

Use delegated administration to assign limited admin privileges to users in your org who aren't administrators. For example, let's say you want the Customer Support team manager to manage users in the Support Manager role and all subordinate roles. Create a delegated admin for this purpose so that you can focus on other administration tasks.

Delegated administrators can:

- Create and edit users in specified roles and all subordinate roles. User editing tasks include resetting passwords, setting quotas, creating default opportunity teams, and creating personal groups for those users.
- Unlock users.
- Assign users to specified profiles.
- Assign or remove permission sets for users in their delegated groups.
- Assign or remove permission set groups for users in their delegated groups.
- Create public groups and manage membership in specified public groups.
- Log in as a user who has granted login access to the administrator.
- Manage custom objects and customize nearly every aspect of a custom object. However, a delegated admin can't create or modify relationships on the object or set org-wide sharing defaults.
- Administer users across all delegated groups to which the delegated admin is assigned. For example, Sam Smith is specified as a delegated administrator in two delegated groups, Group A and Group B. Sam can assign a permission set or public group from Group A to users in Group B.



Note: When delegating administration, keep the following in mind. Delegated administrators:

- Can't assign profiles or permission sets with the "Modify All Data" permission
- Don't see the None Specified option when selecting a role for new users

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To manage delegated administration:

- **Customize Application**

To be a delegated administrator:

- **View Setup and Configuration**

- Need access to custom objects to access the merge fields on those objects from formulas
- Can't modify permission sets
- Must be assigned the "Manage Roles" permission to change the role of portal account owners

To delegate administration of particular objects, use object permissions, such as "View All" and "Modify All," instead.

Define Delegate Administrators

Enable delegated administrators to manage users in specified roles and all subordinate roles. You can assign specified profiles to those users, and log in as users who have granted login access to administrators. A delegated administration group is a group of users who have the same admin privileges. These groups are not related to public groups used for sharing.

You cannot delegate administrative duties related to your org to partner portal or Customer Portal users. However, you can delegate some portal administrative duties to portal users. Before you begin, ensure that roles are assigned to the delegated group so that the delegated administrator can manage group permissions.

1. From Setup, enter *Delegated Administration* in the **Quick Find** box, then select **Delegated Administration** and click **New**.
2. Select or create a delegated group.
3. To allow group users to log in as users in the role hierarchy that they administer, select **Enable Group for Login Access**. Depending on your org settings, individual users first grant login access to allow their administrators to log in as them.
4. Click **Save**.
5. For each related list, click **Add** to define your delegated group details.

SEE ALSO:

[Delegate Administrative Duties](#)

Topics and Tags Settings

Topics on objects allow users to add topics to records so they can organize them by common themes. With Chatter enabled, users can also see related posts and comments. Enabling topics for an object disables public tags on records of that object type. Personal tags aren't affected.

[Enable Tags](#)

Allow users to add personal or public tags to most records. Tags are words or short phrases that users associate to records to describe and organize data in a personalized way.

[Adding Tags to the Sidebar](#)

When you enable tags for your organization, you can add the Tags component to your users' sidebar.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To manage delegated administration:

- Customize Application

To be a delegated administrator:

- View Setup and Configuration

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Topic and tag settings are available in: **All** Editions

[Delete Personal Tags for Deactivated Users](#)

Your org can have up to 5,000,000 personal and public tags applied to records across all users. If your org is approaching this limit, delete personal tags for deactivated users.

SEE ALSO:

[Configure Topics for Records in Lightning Experience](#)[Enable and Configure Topics for Objects in Salesforce Classic](#)

Enable Tags

Allow users to add personal or public tags to most records. Tags are words or short phrases that users associate to records to describe and organize data in a personalized way.

1. From Setup, enter *Tag Settings* in the *Quick Find* box, then select **Tag Settings**.
2. Select **Enable Personal Tags** and **Enable Public Tags** to allow users to add personal and public tags to records. Deselect both options to disable tags.
3. Specify which objects and page layouts display tags in a tag section at the top of record detail pages. The tag section is the only place where a user can add tags to a record.

For example, if you select only account page layouts, users in your org can only tag account records. If you select only account page layouts for personal tags and not public tags, users can tag account records only with personal tags.

4. Click **Save**.

When enabling tags, keep these guidelines in mind.

- You can also add tags to page layouts by editing a layout directly. However, you can't add tags to feed-based page layouts.
- Search results and the Tags page don't display custom objects without an associated tab, even if tags are enabled for the custom object. If you want custom object records to appear, create an associated tab. The tab doesn't have to be visible to users.
- Customer Portal users can't view the tags section of a page, even if it is included in a page layout.
- When Chatter is disabled, joined reports can't be tagged.

SEE ALSO:

[Topics and Tags Settings](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Tag settings available in: **All Editions**

USER PERMISSIONS

To modify tag settings:

- [Customize Application](#)

Adding Tags to the Sidebar

When you enable tags for your organization, you can add the Tags component to your users' sidebar.

This component allows users to navigate to the Tags page where they can browse, search, and manage their tags. It also lists each user's most recently used tags. To add this component:

1. From Setup, enter *Home Page Layouts* in the **Quick Find** box, then select **Home Page Layouts**.
2. Next to a home page layout that you want to modify, click **Edit**.
3. Select the **Tags** checkbox and click **Next**.
4. Arrange the Tags component on your page layout as desired, and click **Save**.

 **Tip:** If you want the Tags component to appear on all pages and not just the Home tab, from Setup, enter *User Interface* in the **Quick Find** box, then select **User Interface**, and select **Show Custom Sidebar Components on All Pages**.

SEE ALSO:

[Topics and Tags Settings](#)

Delete Personal Tags for Deactivated Users

Your org can have up to 5,000,000 personal and public tags applied to records across all users. If your org is approaching this limit, delete personal tags for deactivated users.

1. From Setup, enter *Personal Tag Cleanup* in the **Quick Find** box, then select **Personal Tag Cleanup**.
2. Select one or more deactivated users and click **Delete**.

You can't restore personal tags after you delete them.

SEE ALSO:

[Topics and Tags Settings](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Tag settings available in: **All Editions**

USER PERMISSIONS

To modify tag settings:

- [Customize Application](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Personal Tag Cleanup available in: **All Editions**

USER PERMISSIONS

To delete personal tags for deactivated users:

- [Customize Application](#)

Manage Data Access

Salesforce provides a flexible, layered data sharing design that lets admins control user access to data. Managing data access enhances security by exposing only data that's relevant to users. Use permission sets, permission set groups, and profiles to control the objects and fields users can access. Use organization-wide sharing settings, user roles, and sharing rules to specify the individual records that users can view and edit.

 **Note:** Looking for info on managing Salesforce org, login, and API access? See [Identify Your Users and Manage Access](#).

Control Who Sees What

Salesforce data sharing lets you expose specific data sets to individuals and groups of users. Permission sets, permission set groups, and profiles provide object-level and field-level security by controlling access. Record-level sharing settings, user roles, and sharing rules control the individual records that users can view and edit.

User Permissions and Access

User permissions and access settings are specified in profiles and permission sets. To use them effectively, understand the differences between profiles and permission sets.

User Access and Permissions Assistant

Streamline your access and permissions management with the User Access and Permissions Assistant. Convert profiles to editable permission sets. Analyze and report on permissions and access in your org. Manage your permission set groups and the permissions that they contain.

User Access Policies (Beta)

With user access policies, you define aggregated access for your users in a single operation. Automate your users' assignments to permission set licenses, permission sets, permission set groups, package licenses, queues, and groups. You can create policies that grant or remove access whenever users are created or updated, or in a one-time manual migration.

Profiles

Profiles define default settings for users. When you create users, you assign a profile to each one.

Permission Sets

A permission set is a collection of settings and permissions that give users access to various tools and functions. Permission sets extend users' functional access without changing their profiles and are the recommended way to manage your users' permissions.

Permission Set Groups

A permission set group streamlines permissions assignment and management. Use a permission set group to bundle permission sets together based on user job personas or roles.

What Is a Group?

A group consists of a set of users. A group can contain individual users, other groups, or the users in a particular role or territory. It can also contain the users in a particular role or territory plus all the users below that role or territory in the hierarchy.

Sharing Settings

In Salesforce, you can control access to data at many different levels. For example, you can control the access your users have to objects with object permissions. Within objects, you can control the access users have to fields using field-level security. To control access to data at the record level, use sharing settings and restriction rules.

Insufficient Privileges Errors

Follow this troubleshooting flowchart if you're encountering an insufficient privileges error.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

The available data management options vary according to which Salesforce edition you have.

Restriction Rules

Restriction rules let you enhance your security by allowing certain users to access only specified records. They prevent users from accessing records that can contain sensitive data or information that isn't essential to their work. Restriction rules filter the records that a user has access to so that they can access only the records that match the criteria you specify.

Scoping Rules

Scoping rules let you control the records that your users see based on criteria that you select. You can set up scoping rules for different users in your Salesforce org so that they can focus on the records that matter to them. Users can switch the set of records they're seeing as needed.

Control Who Sees What

Salesforce data sharing lets you expose specific data sets to individuals and groups of users. Permission sets, permission set groups, and profiles provide object-level and field-level security by controlling access. Record-level sharing settings, user roles, and sharing rules control the individual records that users can view and edit.

Watch how you can control who sees what data in your organization.

 [Watch a video](#)

 **Tip:** When implementing security and sharing rules for your organization, make a table of types of users. Specify the level of access to data required for each type. Indicate the access level for each object and for fields and records within the object. Then refer to this table as you set up your security model.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

The available data management options vary according to which Salesforce Edition you have.

Object-Level Security (Permission Sets and Profiles)

Object-level security—or object permissions—provide the bluntest way to control data access. You can prevent a user from seeing, creating, editing, or deleting any instance of a particular object type, such as a lead or opportunity, by using object permissions. You can hide tabs and objects from selected users, so that they don't even know that type of data exists.

You can specify object permissions in permission sets and profiles. *Permission sets* and *profiles* are collections of settings and permissions that determine what a user can do in the application. The settings are similar to a group in a Windows network, where the members of the group have the same folder permissions and access to the same software.

Typically, profiles are defined by a user's job function, such as Salesforce admin or sales representative. You can assign one profile to many users, but you can assign only one profile per user. You can use permission sets to grant more permissions and access settings to users. Now it's easier to manage users' permissions and access because you can assign multiple permission sets to a single user.

Field-Level Security (Permission Sets and Profiles)

Sometimes you want users to have access to an object while limiting their access to individual fields in that object. Field-level security—or field permissions—control whether a user can see, edit, and delete the value for a particular field on an object. You can protect sensitive fields without hiding the entire object. You also can control field permissions in permission sets and profiles.

Field permissions control the visibility of fields in any part of the app, including related lists, list views, reports, and search results. To ensure that a user can't access a particular field, use field permissions. No other settings provide as much protection for a field. Page layouts only control the visibility of fields on detail and edit pages.

 **Note:** With some exceptions, search results aren't returned for records with fields that an admin or end user can't access because of field level security. For example, a user searches for Las Vegas in Accounts, but doesn't have access to the Account fields Billing Address and Shipping Address. Salesforce does a keyword search, matching the terms Las Vegas, Las, and Vegas in the searchable

fields. No results are returned for records that match only the Billing and Shipping Address fields because the user doesn't have access to these fields. There are some fields that don't enforce field level security and return search results.

Record-Level Security (Sharing)

After setting object- and field-level access permissions, you can configure access settings for records. Record-level security lets you give users access to some object records, but not others. Every record is owned by a user or a queue. The owner has full access to the record. In a hierarchy, users higher in the hierarchy always have the same access to users below them in the hierarchy. This access applies to records owned by users and records shared with them.

To specify record-level security, set your organization-wide sharing settings, define a hierarchy, and create sharing rules.

- Organization-wide sharing settings

The first step in record-level security is to determine the organization-wide sharing settings for each object. Organization-wide sharing settings specify the default level of access that users have to each others' records.

You use organization-wide sharing settings to lock your data to the most restrictive level. Use the other record-level security and sharing tools to selectively give access to other users. For example, users have object-level permissions to read and edit opportunities, and the organization-wide sharing setting is Read-Only. By default, those users can read all opportunity records, but can't edit any unless they own the record or are granted other permissions.

- Role hierarchy

After you specify organization-wide sharing settings, the first way to give wider access to records is with a role hierarchy. Similar to an organization chart, a role hierarchy is the level of data access that a user or group of users needs. The role hierarchy ensures that users higher in the hierarchy can always access the same data as users who are lower, regardless of the organization-wide default settings. Each role in the hierarchy can represent a level of data access that a user or group of users needs rather than matching your organization chart.

Similarly, you can use a territory hierarchy to share access to records. See [Define Default User Access for Territory Records](#).



Note: Although it's easy to confuse permission sets and profiles with roles, they control two different things. Permission sets and profiles control a user's object and field access permissions. Roles primarily control a user's record-level access through role hierarchy and sharing rules.

- Sharing rules

With sharing rules you can make automatic exceptions to organization-wide sharing settings for sets of users. Use sharing rules to give these users access to records they don't own or can't normally see. Sharing rules, like role hierarchies, are only used to give more users access to records—they can't be stricter than your organization-wide default settings.

- Manual sharing

Sometimes it's impossible to define a consistent group of users who need access to a particular set of records. Record owners can use manual sharing to give read and edit permissions to users who don't have access any other way. Manual sharing isn't automated like organization-wide sharing settings, role hierarchies, or sharing rules. But it gives record owners the flexibility to share records with users that must see them.

- User sharing

With user sharing, you can show or hide an internal or external user from another user in your organization. User sharing rules are based on membership to a public group, role, or territory, so you must create the appropriate public groups, roles, or territories before creating user sharing rules. Each sharing rule shares members of a source group with members of the target group. Users inherit the same access as users below them in the role hierarchy.

- Apex managed sharing

If sharing rules and manual sharing don't provide the required control, you can use Apex managed sharing. Apex managed sharing allows developers to programmatically share custom objects. When you use Apex managed sharing on a custom object, only users with the Modify All Data permission can add or change the sharing on the custom object's record. The sharing access is maintained across record owner changes.

- Restriction rules

When a restriction rule is applied to a user, the data that they had read access to via your sharing settings is further scoped to only records matching the record criteria that you set. This behavior is similar to how you can filter results in a list view or report, except that it's permanent.

- Scoping rules

With scoping rules you can set criteria to help your users see only records that are relevant to them. Scoping rules don't restrict the record access that your users already have. They scope the records that your users see. Your users can still open and report on all records that they have access to per your sharing settings.

SEE ALSO:

[Financial Services Cloud Administrator Guide: Control Who Sees What with Compliant Data Sharing Profiles](#)
[Permission Sets](#)
[Field-Level Security](#)
[Sharing Settings](#)

User Permissions and Access

User permissions and access settings are specified in profiles and permission sets. To use them effectively, understand the differences between profiles and permission sets.

User permissions and access settings specify what users can do within an organization:

- Permissions determine a user's ability to edit an object record, view the Setup menu, permanently delete records in the Recycle Bin, or reset a user's password.
- Access settings determine other functions, such as access to Apex classes, app visibility, and the hours when users can log in.

Every user is assigned only one profile, but can also have multiple permission sets. When determining access for your users, use *profiles to assign the minimum permissions and access settings* for specific groups of users. Then use *permission sets to grant more permissions* as needed.

This table shows the types of permissions and access settings that are specified in profiles and permission sets.

Permission or Setting Type	In Profiles?	In Permission Sets?
Assigned apps	✓	✓
Tab settings	✓	✓
Record type assignments	✓	✓
Page layout assignments	✓	

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

The available permissions and settings vary according to which Salesforce edition you have.

Permission sets available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

Permission or Setting Type	In Profiles?	In Permission Sets?
Object permissions	✓	✓
Field permissions	✓	✓
User permissions (app and system)	✓	✓
Apex class access	✓	✓
Visualforce page access	✓	✓
External data source access	✓	✓
Service provider access (if Salesforce is enabled as an identity provider)	✓	✓
Custom permissions	✓	✓
Login hours	✓	
Login IP ranges	✓	

[Revoke Permissions and Access](#)

You can use profiles and permission sets to grant access but not to deny access. Permissions granted from both profiles and permission sets are honored. For example, if Transfer Record isn't enabled in a profile but is enabled in a permission set, the assigned user can transfer records regardless of whether the user owns them. To revoke a permission, you must remove all instances of the permission from the user.

SEE ALSO:

[Profiles](#)

[Permission Sets](#)

[Revoke Permissions and Access](#)

User Permissions

User permissions specify what tasks users can perform and what features users can access. For example, users with the “View Setup and Configuration” permission can view Setup pages, and users with the “API Enabled” permission can access any Salesforce API.

You can enable user permissions in permission sets and custom profiles. In permission sets and the enhanced profile user interface, these permissions—as well as their descriptions—are listed in the App Permissions or System Permissions pages. In the original profile user interface, user permissions are listed under Administrative Permissions and General User Permissions.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

The user permissions available vary according to which edition you have.

To view permissions and their descriptions, from Setup, enter *Permission Sets* in the **Quick Find** box, then select **Permission Sets**, then select or create a permission set. Then from the Permission Set Overview page, click **App Permissions** or **System Permissions**.

SEE ALSO:

[Profiles](#)

[Permission Sets](#)

[Standard Profiles](#)

Object Permissions

Object permissions specify the base-level access users have to create, read, edit, and delete records for each object. You can manage object permissions in permission sets and profiles.

Object permissions either respect or override sharing rules and settings. The following permissions specify the access that users have to objects.

Permission	Description	Respects or Overrides Sharing?
Read	Users can only view records of this type.	Respects sharing
Create	Users can read and create records.	Respects sharing
Edit	Users can read and update records.	Respects sharing
Delete	Users can read, edit, and delete records.	Respects sharing
View All	Users can view all records associated with this object, regardless of sharing settings.	Overrides sharing
Modify All	Users can read, edit, delete, transfer, and approve all records associated with this object, regardless of sharing settings. “Modify All” on documents allows access to all shared and public folders, but not the ability to edit folder properties or create folders. To edit folder properties and create folders, users must have the “Manage Public Documents” permission.	Overrides sharing

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

 **Note:** A profile or a permission set can have an entity, such as Account, with a master-detail relationship. A broken permission dependency exists if the child entity has permissions that the parent must have. Salesforce updates the parent entity for a broken permission dependency on the first save action for the profile or permission set.

If the child entity has these permissions	These permissions are enabled on the parent entity
Modify All OR View All	View All

If the child entity has these permissions	These permissions are enabled on the parent entity
View All OR Read	Read

SEE ALSO:

[“View All” and “Modify All” Permissions Overview](#)

[Comparing Security Models](#)

[Field Permissions](#)

“View All” and “Modify All” Permissions Overview

The “View All” and “Modify All” permissions ignore sharing rules and settings, allowing administrators to grant access to records associated with a given object across the organization. “View All” and “Modify All” can be better alternatives to the “View All Data” and “Modify All Data” permissions.

Be aware of the following distinctions between the permission types.

Permissions	Used for	Users who need them
View All Modify All	Delegation of object permissions.	Delegated administrators who manage records for specific objects
View All Data Modify All Data	Managing all data in an organization; for example, data cleansing, deduplication, mass deletion, mass transferring, and managing record approvals. Users with View All Data (or Modify All Data) permission can view (or modify) all apps and data, even if the apps and data are not shared with them.	Administrators of an entire organization. If a user requires access only to metadata for deployments, you can enable the Modify Metadata Through Metadata API Functions permission. This permission gives such users the access they need for deployments without providing access to org data. For details, see “Modify Metadata Through Metadata API Functions Permission” in Salesforce Help.
View All Users	Viewing all users in the organization. Grants Read access to all users, so that you can see their user record details, see them in searches, list views, and so on.	Users who need to see all users in the organization. Useful if the organization-wide default for the user object is Private. Administrators with the Manage Users permission are automatically granted the View All Users permission.
View All Lookup Record Names	Viewing record names in all lookup and system fields.	Administrators and users who need to see all information about a record, such as its related records and the Owner, Created By, and Last Modified

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All** Editions

Permissions	Used for	Users who need them
		By fields. This permission only applies to lookup record names in list views and record detail pages.

View All Data, Modify All Data, and View All or Modify All for a given object don't override field-level security. Users must still have field permissions to read or edit each field on an object.

View All and Modify All are not available for ideas, price books, article types, and products.

View All and Modify All allow for delegation of object permissions only. To delegate user administration and custom object administration duties, define delegated administrators.

View All for a given object doesn't automatically give access to its detail objects. In this scenario, users must have Read access granted via sharing to see any associated child records to the parent record.

View All Users is available if your organization has User Sharing, which controls user visibility in the organization.

SEE ALSO:

[Object Permissions](#)

Comparing Security Models

To manage your users' access to data, you can configure sharing settings, permissions, and other features.

Salesforce user security is an intersection of [sharing](#), and [user](#) and [object](#) permissions. In some cases, such as in end-user record level access, it is advantageous to use sharing to provide access to records. In other cases, such as when delegating record administration tasks like transferring records, cleansing data, deduplicating records, mass deleting records, and delegating workflow approval processes, it is advantageous to override sharing and use permissions to provide access to records.

The "Read," "Create," "Edit," and "Delete" permissions respect sharing settings, which control access to data at the record level. The "View All" and "Modify All" permissions override sharing settings for specific objects. Additionally, the "View All Data" and "Modify All Data" permissions override sharing settings for *all* objects.

The following table describes the differences between the security models.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

	Permissions that Respect Sharing	Permissions that Override Sharing
Target audience	End-users	Delegated data administrators
Where managed	"Read," "Create," "Edit," and "Delete" object permissions; Sharing settings	"View All" and "Modify All"
Record access levels	Private, Read-Only, Read/Write, Read/Write/Transfer/Full Access	"View All" and "Modify All"
Ability to transfer	Respects sharing settings, which vary by object	Available on all objects with "Modify All"

	Permissions that Respect Sharing	Permissions that Override Sharing
Ability to approve records, or edit and unlock records in an approval process	None	Available on all objects with “Modify All”
Ability to report on all records	Available with a sharing rule that states: the records owned by the public group “Entire Organization” are shared with a specified group, with Read-Only access	Available on all objects with “View All”
Object support	Available on all objects except products, documents, solutions, ideas, notes, and attachments	Available on most objects via object permissions. View All and Modify All are not available for ideas, price books, article types, and products.
Group access levels determined by	Roles, Roles and Subordinates, Roles and Internal Subordinates, Roles, Internal and Portal Subordinates, Queues, Teams, and Public Groups	Profile or permission sets
Private record access	Not available	Available on private contacts, opportunities, and notes and attachments with “View All” and “Modify All”
Ability to manually share records	Available to the record owner and any user above the record owner in the role hierarchy	Available on all objects with “Modify All”
Ability to manage all case comments	Not available	Available with “Modify All” on cases

Field Permissions

Field permissions specify the access level for each field in an object. In permission sets and the enhanced profile user interface, the setting labels differ from those in the original profile user interface and in field-level security pages for customizing fields.

Access Level	Enabled Settings in Permission Sets and Enhanced Profile User Interface	Enabled Settings in Original Profile and Field-Level Security Interfaces
Users can read and edit the field.	Read and Edit	Visible
Users can read but not edit the field.	Read	Visible and Read-Only

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

Access Level	Enabled Settings in Permission Sets and Enhanced Profile User Interface	Enabled Settings in Original Profile and Field-Level Security Interfaces
Users can't read or edit the field.	None	None

SEE ALSO:

[Field-Level Security](#)[Object Permissions](#)

Permission Set and Permission Set Group Assignment Expiration

Use the assignment expiration option to determine the effective time period that users receive access to permissions. When the assignment expires, assigned users no longer have access to the permissions in the permission sets or permission set groups.

Let's say that consultants must access the Contracts object, but they only need access for the duration of a project. Assign the permissions to affected users via permission sets and permission set groups, and select the assignment expiration date and time.

SEE ALSO:

[Set Assignment Expiration Details for Users in Permission Sets and Permission Set Groups](#)[Manage Assignment Expiration Details for Users in Permission Sets and Permission Set Groups](#)[Remove User Assignments in Permission Sets and Permission Set Groups](#)[Permission Assignment Expiration Considerations](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

Set Assignment Expiration Details for Users in Permission Sets and Permission Set Groups

Set assignment expiration dates and assign permissions that expire to users via permission sets and permission set groups. Assigned users receive access to all aggregate permissions until the expiration date.

To assign users to permission set groups, create the permission set group with the permission sets and permissions that you want to assign to users before you begin.

- To activate this feature, enable **Permission Set & Permission Set Group Assignments with Expiration Dates** in User Management Settings.
- Access the Permission Sets or Permission Set Groups Setup page.
 - To edit a permission set, from Setup, in the Quick Find box, enter *Permission Sets*, and then select **Permission Sets**.
 - To edit a permission set group, from Setup, in the Quick Find box, enter *Permission Set Groups*, and then select **Permission Set Groups**.
- In the list view, click the name of the permission set or permission set group name that you want to update.

 **Note:** If a permission set or permission set group contains any of the following permissions, it can't have an expiration date associated with it:

- Assign Permission Set

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To assign a permission set:

- Assign Permission Sets

To enable the beta:

- Customize Application

- Manage Profiles
- Manage Users
- Permission Sets

4. Click **Manage Assignments**.
5. On the Current Assignments page, click **Add Assignment**.
6. Optionally, select or create a list view to refine your user list.
7. Select the users that you want to assign, and click **Next**.
Search for a name by typing it in the search bar.
8. Select an assignment expiration option for the users you selected.
 - a. If you don't want the assignments to expire, select **No expiration date**.
 - b. To choose an expiration date and time zone, select **Specify the expiration date**.

Full Name	Role	Profile	Active	User License	Current Expiration...	New Expiration Date	Time Zone
Erika Turner	Standard User	Standard User	✓	Salesforce	Aug 29, 2021	Aug 31, 2021	America/Los Angeles

- c. Click a time frame, such as 30 days, or to enter a custom date, click **Custom Date**.
 - d. Select a time zone. Assignments expire at 11:59 PM on the date and in the time zone that you specify.
If you select **My Local Time Zone**, expiration occurs at 11:59 PM in your time zone. For example, if you have a user with an assigned expiration who uses Japan Standard Time. You use Pacific Daylight Time as your time zone. If you select **My Local Time Zone** as the time zone expiration option, the user's assignment expires at 11:59 PM Pacific Daylight Time.
9. Click **Assign**.

Example: Suppose you need consultants in the San Francisco office to evaluate language used in sales contracts. Assign the consultants to a permission set group that contains the permissions that they need. When you assign the consultants to the group, specify that the assignment expires in 30 days (GMT-07:00) Pacific Daylight Time (America/Los Angeles). If you assign the permissions on June 1, the assignments expire on June 30 at 11:59 PM Pacific Time.

When you have permission set groups with user assignments that expire, you can make updates to the permission sets in the group. If you update the permission sets by adding or removing permissions, the assigned users receive or lose permissions after the permission

set group recalculation occurs. When the assignment expiration date is reached, assigned users lose access to the permissions in the group.

SEE ALSO:

- [Permission Set and Permission Set Group Assignment Expiration](#)
- [Manage Assignment Expiration Details for Users in Permission Sets and Permission Set Groups](#)
- [Remove User Assignments in Permission Sets and Permission Set Groups](#)
- [Permission Assignment Expiration Considerations](#)

Manage Assignment Expiration Details for Users in Permission Sets and Permission Set Groups

Update or remove assignment expiration dates permission sets and permission set groups.

1. Access the Permission Sets or Permission Set Groups Setup page.
 - a. To edit a permission set, from Setup, in the Quick Find box, enter *Permission Sets*, and then select **Permission Sets**.
 - b. To edit a permission set group, from Setup, in the Quick Find box, enter *Permission Set Groups*, and then select **Permission Set Groups**.
2. In the list view, click the name of the permission set or permission set group name that you want to update.
3. Click **Manage Assignments**.
4. Select the assignments to modify.
5. To modify the selected assignments, click .
 - a. If you don't want the assignments to expire, select **No expiration date**.
 - b. To choose an expiration date and time zone, select **Specify the expiration date**.
 - c. Click a time frame, such as 30 days, or to enter a custom date, click **Custom Date**.
 - d. Select a time zone. Assignments expire at 11:59 PM on the date and in the time zone that you specify.

If you select **My Local Time Zone**, expiration occurs at 11:59 PM in your time zone. For example, if you have a user with an assigned expiration who uses Japan Standard Time. You use Pacific Daylight Time as your time zone. If you select **My Local Time Zone** as the time zone expiration option, the user's assignment expires at 11:59 PM Pacific Daylight Time.

6. Select **Assign**.

SEE ALSO:

- [Permission Set and Permission Set Group Assignment Expiration](#)
- [Set Assignment Expiration Details for Users in Permission Sets and Permission Set Groups](#)
- [Remove User Assignments in Permission Sets and Permission Set Groups](#)
- [Permission Assignment Expiration Considerations](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To assign a permission set:

- [Assign Permission Sets](#)

Remove User Assignments in Permission Sets and Permission Set Groups

Remove user assignments from permission sets and permission set groups.

1. Access the Permission Sets or Permission Set Groups Setup page.
 - a. To edit a permission set, from Setup, in the Quick Find box, enter *Permission Sets*, and then select **Permission Sets**.
 - b. To edit a permission set group, from Setup, in the Quick Find box, enter *Permission Set Groups*, and then select **Permission Set Groups**.
2. In the list view, click the name of the permission set or permission set group name that you want to update.
3. To remove the user, select **Manage Assignments**.
4. Select the assignments to remove.
5. To remove the selected assignments, click .
6. Click **Remove**.

SEE ALSO:

[Permission Set and Permission Set Group Assignment Expiration](#)
[Set Assignment Expiration Details for Users in Permission Sets and Permission Set Groups](#)
[Manage Assignment Expiration Details for Users in Permission Sets and Permission Set Groups](#)
[Permission Assignment Expiration Considerations](#)

Permission Assignment Expiration Considerations

When working with permission assignments that expire, keep these considerations in mind.

- When a permission assign expires, permissions assigned to users via non-expiring permission sets, permission set groups, or through a profile still apply.
 Let's say that you assign a user to a permission set group that includes create permissions on the Contracts object. The user's assignment to the group expires in a week. The user also has create permissions on the Contracts object via a permission set that doesn't expire. When the permission set group assignment expires in a week, the user still has create abilities on the Contracts object via the permission set.
- SOQL queries don't return user assignment information for permission assignments that expire. Assignments that expire are treated as soft-deletes. You can retrieve the expiring assignment information using the `ALL ROWS` clause.
- When an assignment expires, the user remains assigned to the permission set or permission set group. However, the user can't access the permissions associated with the permission set or permission set group.

SEE ALSO:

[Permission Set and Permission Set Group Assignment Expiration](#)
[Manage Assignment Expiration Details for Users in Permission Sets and Permission Set Groups](#)
[Remove User Assignments in Permission Sets and Permission Set Groups](#)
[Set Assignment Expiration Details for Users in Permission Sets and Permission Set Groups](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To assign a permission set:

- [Assign Permission Sets](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

Revoke Permissions and Access

You can use profiles and permission sets to grant access but not to deny access. Permissions granted from both profiles and permission sets are honored. For example, if Transfer Record isn't enabled in a profile but is enabled in a permission set, the assigned user can transfer records regardless of whether the user owns them. To revoke a permission, you must remove all instances of the permission from the user.

Action	Consequence
Disable a permission or remove an access setting in the profile and any permission sets that are assigned to the user.	The permission or access setting is disabled for all other users assigned to the profile or permission sets.
If a permission or access setting is enabled in the user's profile, assign a different profile to the user.	The user may lose other permissions or access settings associated with the profile or permission sets.
AND	
If the permission or access setting is enabled in any permission sets that are assigned to the user, remove the permission set assignments from the user.	

To resolve the consequence in either case, consider all possible options. For example, you can clone the assigned profile or any assigned permission sets where the permission or access setting is enabled. Then, disable the permission or access setting, and assign the cloned profile or permission sets to the user. Another option is use muting permission sets in permission set groups to mute selected permissions for the users assigned to the permission set group.

When possible, we recommend that you use permission sets and permission set groups to manage your users' permissions. Because you can reuse smaller permission set building blocks, you can avoid creating dozens or even hundreds of profiles for each user and job function.

SEE ALSO:

[User Permissions and Access](#)

[Assign Permission Sets to a Single User](#)

User Access and Permissions Assistant

Streamline your access and permissions management with the User Access and Permissions Assistant. Convert profiles to editable permission sets. Analyze and report on permissions and access in your org. Manage your permission set groups and the permissions that they contain.

To use the User Access and Permissions Assistant, you need these permission sets.

- User Access & Permissions Assistant Access
- The permission set to grant access to the Tooling API Credential, which is created during installation
- Optionally, the permission set to assign permissions to access and run the User Access and Permissions Assistant

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

EDITIONS

Available in: all editions except **Starter**

[Install the User Access and Permissions Assistant](#)

To use the User Access and Permissions Assistant, enable the Tooling API. Then download the app from AppExchange, and assign the packaged permission set that comes with the app.

[Analyze Your Permission Assignments](#)

Review your org's permission assignments to quickly determine the permissions that a user has and the configuration that grants a specific permission.

[Converting Profiles to Permission Sets](#)

If your custom or standard profiles have a Salesforce license, you can convert them into a permission set that you can edit and assign.

[Report on Permission Assignments by User](#)

Create a report of which users are assigned a given permission.

[Manage Permission Set Groups](#)

Use the User Access and Permissions Assistant to create, modify, or remove permission set groups. You can also assign or unassign permission set groups and add or remove permission sets to groups.

[User Access and Permissions Assistant Considerations](#)

Be aware of these considerations and special behaviors for the User Access and Permissions Assistant.

Install the User Access and Permissions Assistant

To use the User Access and Permissions Assistant, enable the Tooling API. Then download the app from AppExchange, and assign the packaged permission set that comes with the app.

Be sure to complete the tasks to enable the Tooling API before installing the app. After you enable the Tooling API, complete the app installation.

EDITIONS

Available in: all editions

[Create a Connected App for the Tooling API](#)

Create a new connected app for the User Access and Permissions Assistant.

[Create an Authentication Provider for the Tooling API](#)

Create an authentication provider to facilitate authentication with Salesforce.

[Update the Callback URL in the Connected App](#)

Update the value of the callback URL in the connected app to use the value from the authentication provider.

[Create a Named Credential for the Tooling API](#)

To work correctly, the credential that you create must have the API name Tooling_API_Credential.

[Create a Permission Set to Use the Named Credential](#)

Create a custom permission set to enable users to use the Tooling API for the User Access and Permissions Assistant. You can assign this permission set to any users who use the app.

[Download the User Access and Permissions Assistant Package](#)

Download the User Access and Permissions Assistant from AppExchange.

[Assign the Helper App Access Permission Set](#)

For access to the User Access and Permissions Assistant, assign the User Access & Permissions Assistant Access permission set.

[Create a Permission Set with Required Permissions for the User Access and Permissions Assistant](#)

Create a permission set to assign to users so that they can use the User Access and Permissions Assistant. These permissions are included in the System Admin standard profile. Users with that profile don't require access to this permission step.

Set User Authentication for the Tooling API Credential

Set your user account to use the Tooling API Named Credential for authentication.

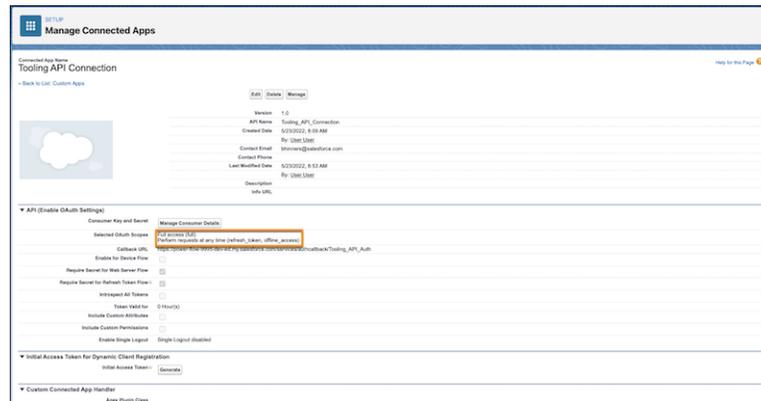
Create a Connected App for the Tooling API

Create a new connected app for the User Access and Permissions Assistant.

1. In Setup, in the Quick Find box, enter *Apps*, and then select **App Manager**.
2. In Lightning, click **New Connected App**. In Classic, click **New**.
3. Complete the required fields for Connected App.
4. Select **Enable OAuth Settings**.
 - a. For Callback URL, temporarily enter *https://login.salesforce.com*. You change this URL in a later task.
 - b. For Selected OAuth Scopes, add: *Full access (full)* and *Perform requests at any time (refresh_token, offline_access)*.
5. Save your changes.
6. Click **Manage Consumer Details**.

 **Example:**

Connected App Example with OAuth Scopes Highlighted



The screenshot shows the 'Manage Connected Apps' interface in Salesforce. The main heading is 'Tooling API Connection'. Below this, there are several sections:

- API (Enable OAuth Settings):** This section contains several fields:
 - Selected OAuth Scopes:** This field is highlighted with an orange box and contains the text: 'Full access (full)' and 'Perform requests at any time (refresh_token, offline_access)'. A 'Manage Consumer Details' link is visible to the right of this field.
 - Callback URL:** A text field containing 'https://login.salesforce.com'.
 - Enable for Device Flow:** A checkbox that is currently unchecked.
 - Require Secret for Web Server Flow:** A checkbox that is currently unchecked.
 - Require Secret for Native Mobile Flow:** A checkbox that is currently unchecked.
 - Introspect All Tokens:** A checkbox that is currently unchecked.
 - Token Valid for:** A dropdown menu set to '0 Hours'.
 - Include Custom Attributes:** A checkbox that is currently unchecked.
 - Include Custom Permissions:** A checkbox that is currently unchecked.
 - Enable Single Logout:** A checkbox that is currently unchecked.
- Initial Access Token for Dynamic Client Registration:** A section with a text field and a 'Generate' button.
- Custom Connected App Handler:** A section with a text field and an 'Add Plugin Class' button.

Have the Consumer Key and Consumer Secret values ready for creating an authentication provider, then continue to [Create an Authentication Provider for the Tooling API](#) on page 488.

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To create connected apps:

- Customize Application AND either Modify All Data OR Manage Connected Apps

Create an Authentication Provider for the Tooling API

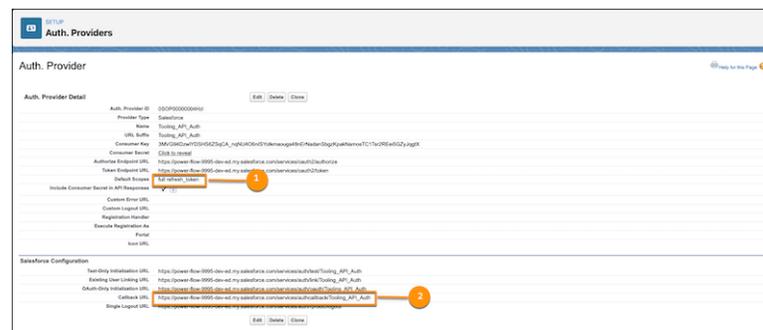
Create an authentication provider to facilitate authentication with Salesforce.

Before you complete this task, [Create a Connected App for the Tooling API](#) on page 487.

1. Open Setup in a separate tab from the previous task.
2. In the Quick Find box, enter *Auth. Providers*, and select that option.
3. Click **New**.
4. Select Salesforce as the Provider Type.
5. Complete the required fields.
 - a. Set the Consumer Key and Consumer secret using the values from the Create a Connected App for the Tooling API task.
 - b. Set the Default Scopes to: *refresh_token full*
6. Save your changes.
7. Copy the value of the Callback URL.

 **Example:**

Authentication Provider Example with Scopes and Callback URL Highlighted



(1) the Default Scopes. (2) the Callback URL value to copy.

With the value of the Callback URL in the authentication provider, update the callback URL in the connected app. Continue to [Update the Callback URL in the Connected App](#) on page 489.

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To create authentication providers

- Customize Application AND Manage Auth. Providers

Update the Callback URL in the Connected App

Update the value of the callback URL in the connected app to use the value from the authentication provider.

To complete this task, you need the value of the callback URL in the authentication provider created in the [Create an Authentication Provider for the Tooling API](#) on page 488 task.

When you created the connected app in the [Create a Connected App for the Tooling API](#) on page 487 task, the value of the callback URL was a placeholder. To use the correct value, you update it in this step.

1. In Setup, in the Quick Find box, enter *Apps*, and then select **App Manager**.
2. In the entry for the connected app that you created, select **View** from the dropdown on the far right.
3. Click **Edit**.
4. To create an authentication provider, update the callback URL to use the value from the previous task.
5. Save your changes.

Continue to [Create a Named Credential for the Tooling API](#) on page 489.

Create a Named Credential for the Tooling API

To work correctly, the credential that you create must have the API name `Tooling_API_Credential`.

To complete this task, you need the value of the callback URL in the authentication provider created in the [Create an Authentication Provider for the Tooling API](#) task.

1. From Setup, in the Quick Find box, enter *Named Credentials*, and then select it.
2. Click the dropdown next to **New** and select **New Legacy**.
3. Enter the values:
 - a. Label: *Tooling API Credential*
 - b. Name: Auto-populates as `Tooling_API_Credential`
 - c. URL: The domain from the callback URL that shows in the authentication provider. For example, if the callback URL is `https://www.example.com/services/authcallback/PermhelperAuth`, then the domain is `https://www.example.com`.
 - d. Identity Type: Per User
 - e. Authentication Protocol: OAuth 2.0
 - f. Authentication Provider: The authentication provider created in the [Create an Authentication Provider for the Tooling API](#) task.
 - g. Scope: *refresh_token full*
4. Select the Callout Options.
 - a. Select the checkboxes for Generate Authorization Header and Allow Merge Fields in HTTP Body. Leave the other fields blank.
5. Save your changes.
You're prompted to log into your org.
6. Log in at the prompt.
7. At the connected app authorization screen, click **Allow**.

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To modify connected apps:

- Customize Application AND either *Modify All Data* OR *Manage Connected Apps*

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

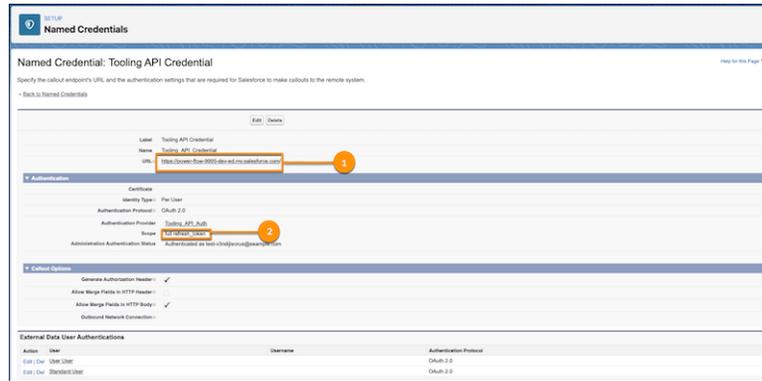
To create named credentials

- Customize Applications

When you're redirected back to the Named Credential screen, the Administration Authentication Status field shows Authenticated as (your login).

 **Example:**

Named Credential Example with URL and Scope Highlighted



The screenshot shows the 'Named Credential: Tooling API Credential' configuration page. The URL field is highlighted with a red box and a '1' callout, and the Scope field is highlighted with a red box and a '2' callout.

(1) The URL with the domain value. (2) The scope.

Continue to [Create a Permission Set to Use the Named Credential](#) on page 490.

Create a Permission Set to Use the Named Credential

Create a custom permission set to enable users to use the Tooling API for the User Access and Permissions Assistant. You can assign this permission set to any users who use the app.

Before you complete this task, complete the [Create a Connected App for the Tooling API](#) and [Create a Named Credential for the Tooling API](#) tasks.

1. From Setup, in the Quick Find box, enter *permission*, and then select **Permission Sets**.
2. Click **New**.
3. Enter a label and API name, and then save.
4. On the page for your new permission set, select Named Credential Access.
5. Click **Edit**.
6. Select Tooling_API_Credential, and add it to the Enabled Named Credentials.
7. Save your changes.
8. Navigate to the permission set page, and then select Assigned Connected Apps.
9. Click **Edit**.
10. Select the connected app that you created previously, and add it to Enabled Connected Apps.
11. Save your changes.

You're now ready to install the app! Continue to [Download the App from Appexchange](#).

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To create permission sets

- Manage Profiles and Permission Sets

Download the User Access and Permissions Assistant Package

Download the User Access and Permissions Assistant from AppExchange.

1. Log in with your Trailhead email, and navigate to the listing on [AppExchange](#).
2. Select **Get it Now**, and from the dropdown, select the org that you want to install it in.
3. Agree to the terms and conditions.
4. After you're redirected to the Salesforce login page, input the credentials for the Salesforce org that you want to install the solution in.
5. Select the profiles that you want to access the solution: Admins Only, Everyone, or a specific profile.

Assign the Helper App Access Permission Set

For access to the User Access and Permissions Assistant, assign the User Access & Permissions Assistant Access permission set.

The User Access & Permissions Assistant Access permission set grants access to the User Access and Permissions Assistant.

1. From Setup, in the Quick Find box, enter *users*, and then select **Users**.
2. Select the users to assign the permission set.
3. In the Permission Set Assignments related list, click **Edit Assignments**.
4. Optionally, if you created a permission set to assign administrative permissions for Assistant, select that under Available Permission Sets, and click **Add**.
5. Save your work.

Create a Permission Set with Required Permissions for the User Access and Permissions Assistant

Create a permission set to assign to users so that they can use the User Access and Permissions Assistant. These permissions are included in the System Admin standard profile. Users with that profile don't require access to this permission step.

1. From Setup, in the Quick Find box, enter *permission*, and then select **Permission Sets**.
2. Click **New**.
3. Enter a label and API name, and then save.
4. On the page for your new permission set, select System Permissions.
5. Click **Edit**.
6. Enable these permissions.
 - a. API Enabled
 - b. Assign Permission Sets
 - c. Customize Application
 - d. Manage Custom Permissions
 - e. Manage Profiles and Permission Sets
 - f. Manage Session Permission Set Activations

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To install packages:

- Download AppExchange Packages

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To assign permission sets:

- Assign Permission Sets AND View Setup and Configuration

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To create permission sets:

- Manage Profiles and Permission Sets

- g. View Roles and Role Hierarchy
 - h. View Setup and Configuration
7. Save your work.

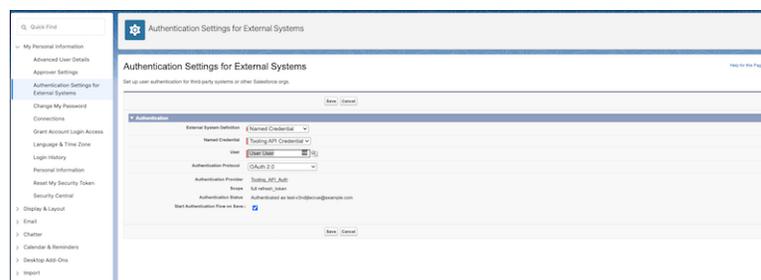
Set User Authentication for the Tooling API Credential

Set your user account to use the Tooling API Named Credential for authentication.

1. In the upper right corner, access your personal settings.
 - a. In Lightning, click your image.
 - b. In Classic, click the down arrow next to your name, and select **Setup**.
2. In the Quick Find box, enter *Authentication*, and then select **Authentication Settings for External Systems**.
3. Click **New**.
4. Complete the fields.
 - a. External System Definition: Named Credential
 - b. Named Credential: Tooling API Credential
 - c. User: Select your username.
 - d. Authentication Protocol: OAuth 2.0
 - e. Select **Start Authentication Flow on Save**
5. Save your work.

 **Example:**

Example of Authentication Settings for External Systems



Analyze Your Permission Assignments

Review your org's permission assignments to quickly determine the permissions that a user has and the configuration that grants a specific permission.

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To store authentication settings for a named credential:

- The named credential enabled under Named Credential Access

To edit another user's authentication settings for external systems:

- Manage Users

Analyze User Permissions

Find the permissions assigned to the selected user.

Permission Sets Needed

To access the User Access and Permissions Assistant: User Access & Permissions Assistant Access

1. In the User Access and Permissions Assistant, select Permissions Analyzer.
2. Under **Analyze by**, select **User**.
3. Enter or search for a user.
4. Optionally, to filter the list of associated permission sets, enter a permission set name.
5. In the results, select the permissions to review. To see permission origin information, click  next to the entry.

Analyze Object Permissions

Find the permission types that are assigned to your selected object.

Permission Sets Needed

To access the User Access and Permissions Assistant: User Access & Permissions Assistant Access

1. In the User Access and Permissions Assistant, select Permissions Analyzer.
2. In the Analyze by picklist, select **Permission**.
3. In the Object picklist, select the object type to search on.
4. In the Permission picklist, select the permission type to filter on.

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To use the User Access and Permissions Assistant:

- API Enabled AND Assign Permission Sets AND Customize Application AND Manage Custom Permissions AND Manage Profiles and Permission Sets AND Manage Session Permission Set Activations AND View Roles and Role Hierarchy AND View Setup and Configuration

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To use the User Access and Permissions Assistant:

- API Enabled AND Assign Permission Sets AND Customize Application AND Manage Custom Permissions AND Manage Profiles and Permission Sets AND Manage Session Permission Set Activations AND View Roles and Role Hierarchy AND View Setup and Configuration

Analyze Permission Set Groups

Find details about permission set groups.

Permission Sets Needed

To access the User Access and Permissions Assistant: User Access & Permissions Assistant Access

1. In the User Access and Permissions Assistant, select Permissions Analyzer.
2. In the Analyze by picklist, select **Permission Set Groups**.
3. For each permission set group that you want to analyze, select View Details.
 - a. To view all permissions associated with the permission set group, select **Combined Permissions**. Filter by enabled or muted permissions, or both.
 - b. To view details about the permission sets included in the permission set group, select **Permission Sets**.
 - c. To view users who are assigned this permission set group and details about them, select **Assigned Users**.

Converting Profiles to Permission Sets

If your custom or standard profiles have a Salesforce license, you can convert them into a permission set that you can edit and assign.

Some profile features aren't supported in permission sets and don't convert.

- Defaults such as Default Apps, Default Tabs, Default Record Types
- Page Layout Assignments
- Login IP Ranges/Login Settings

[Convert a Profile to a Permission Set](#)

Convert a profile to an editable permission set.

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To use the User Access and Permissions Assistant:

- API Enabled AND Assign Permission Sets AND Customize Application AND Manage Custom Permissions AND Manage Profiles and Permission Sets AND Manage Session Permission Set Activations AND View Roles and Role Hierarchy AND View Setup and Configuration

EDITIONS

Available in: all editions except **Starter**

Convert a Profile to a Permission Set

Convert a profile to an editable permission set.

Permission Sets Needed

To access the User Access and Permissions Assistant: User Access & Permissions Assistant Access

1. In User Access and Permissions Assistant, select **Converter**.
2. Select the profile to convert.
3. Select **Convert to Permission Set**.
4. Name the permission set.
Record types and tab access aren't included in the conversion.
5. To view the conversion's status, click **View Batch Jobs**.
6. To view the new permission set, click **View Permission Set**.

Report on Permission Assignments by User

Create a report of which users are assigned a given permission.

Permission Sets Needed

To access the User Access and Permissions Assistant: User Access & Permissions Assistant Access

1. In the User Access and Permissions Assistant, select **Report**.
2. Select the permission to report on. These permission types are available.
 - a. User Permissions
 - b. Object Permissions
 - c. Field Permissions
3. Optionally, filter on the user attributes to narrow your report results.
4. Click **Run Report**. The report returns a maximum of 5,000 rows.
5. To export as a CSV file, click **Export Report**. The currently displayed rows are exported, up to a maximum of 100 rows.

 **Note:** To add additional filters, you must reload the page and reselect the permission to report on.

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To use the User Access and Permissions Assistant:

- API Enabled AND Assign Permission Sets AND Customize Application AND Manage Custom Permissions AND Manage Profiles and Permission Sets AND Manage Session Permission Set Activations AND View Roles and Role Hierarchy AND View Setup and Configuration

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To use the User Access and Permissions Assistant:

- API Enabled AND Assign Permission Sets AND Customize Application AND Manage Custom Permissions AND Manage Profiles and Permission Sets AND Manage Session Permission Set Activations AND View Roles and Role Hierarchy AND View Setup and Configuration

Manage Permission Set Groups

Use the User Access and Permissions Assistant to create, modify, or remove permission set groups. You can also assign or unassign permission set groups and add or remove permission sets to groups.

With the User Access and Permissions Assistant, you can:

[Assign or Unassign Permission Set Groups](#)

Assign or unassign permission set groups to users with the User Access and Permissions Assistant.

[Create a Permission Set Group with the User Access and Permissions Assistant](#)

Create a permission set group with the User Access and Permissions Assistant.

[Modify a Permission Set Group with the User Access and Permissions Assistant](#)

Edit the details of a permission set group with the User Access and Permissions Assistant.

[Mute Permissions in a Permission Set Group](#)

Mute permissions in a permission set group with the User Access and Permissions Assistant.

[Add or Remove Permission Sets from a Permission Set Group](#)

With the User Access and Permissions Assistant, you can add a permission set to, or remove a permission set from, a permission set group.

EDITIONS

Available in: all editions except **Starter**

Assign or Unassign Permission Set Groups

Assign or unassign permission set groups to users with the User Access and Permissions Assistant.

Permission Sets Needed

To access the User Access and Permissions Assistant:	User Access & Permissions Assistant Access
--	--

1. In the User Access and Permissions Assistant, select **Manage**.
2. Select Assignments.
3. Select based on the assignment action.
 - a. To assign a permission set group, select **Assign Permission Set Groups to Users**.
 - b. To unassign a permission set group, select **Unassign Permission Set Groups from Users**.
4. Select the users to receive permission set group assignments or have the groups unassigned.
5. Click **Next**.
6. Finalize the action.
 - a. To assign the permission set group, click **Assign**.
 - b. To unassign the permission set group, click **Unassign**.

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To use the User Access and Permissions Assistant:

- API Enabled AND Assign Permission Sets AND Customize Application AND Manage Custom Permissions AND Manage Profiles and Permission Sets AND Manage Session Permission Set Activations AND View Roles and Role Hierarchy AND View Setup and Configuration

Create a Permission Set Group with the User Access and Permissions Assistant

Create a permission set group with the User Access and Permissions Assistant.

Permission Sets Needed

To access the User Access and Permissions Assistant: User Access & Permissions Assistant Access

1. In the User Access and Permissions Assistant, select **Manage**.
2. Click **Create Permission Set Group**.
3. Enter a label and an API name. The API name auto-populates.
4. Optionally, enter a description, and click **Next**.
5. From the Available Permission Sets, select the permission sets to add to the group, then click **Next**.
6. Click **Finish**.

Users are added to a permission set group when the group status is Updated.

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To use the User Access and Permissions Assistant:

- API Enabled AND Assign Permission Sets AND Customize Application AND Manage Custom Permissions AND Manage Profiles and Permission Sets AND Manage Session Permission Set Activations AND View Roles and Role Hierarchy AND View Setup and Configuration

Modify a Permission Set Group with the User Access and Permissions Assistant

Edit the details of a permission set group with the User Access and Permissions Assistant.

Permission Sets Needed

To access the User Access and Permissions Assistant: User Access & Permissions Assistant Access

1. In the User Access and Permissions Assistant, select **Manage**.
2. From the picklist for the selected entry, select **View Permission Set Group**.
3. Select the action to perform.
 - a. To edit the permission set group, click **Edit**.
 - b. To clone the permission set group, click **Clone**.
 - c. To delete the permission set group, click **Delete**.
4. If editing or cloning the permission set group, modify or add a name, API name, and description as needed.
5. To save an edit or clone, click **Save**. To confirm deletion, click **Delete**.

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To use the User Access and Permissions Assistant:

- API Enabled AND Assign Permission Sets AND Customize Application AND Manage Custom Permissions AND Manage Profiles and Permission Sets AND Manage Session Permission Set Activations AND View Roles and Role Hierarchy AND View Setup and Configuration

Mute Permissions in a Permission Set Group

Mute permissions in a permission set group with the User Access and Permissions Assistant.

Permission Sets Needed

To access the User Access and Permissions Assistant: User Access & Permissions Assistant Access

1. In the User Access and Permissions Assistant, select **Manage**.
2. From the picklist for the selected entry, select **View Permission Set Group**.
3. Click **Mute Permissions**.
4. Next to each permission to mute, select the checkbox.
5. Save your work.

Add or Remove Permission Sets from a Permission Set Group

With the User Access and Permissions Assistant, you can add a permission set to, or remove a permission set from, a permission set group.

Permission Sets Needed

To access the User Access and Permissions Assistant: User Access & Permissions Assistant Access

1. In the User Access and Permissions Assistant, select **Manage**.
2. From the picklist for the selected entry, select **View Permission Set Group**.
3. Select **Permission Sets**.
4. Select your action.
 - a. To assign a permission set, click **Assign Permission Sets**.
 - b. To unassign a permission set, click , then confirm.
5. To assign permission sets, select each permission set to add to the list, then click **Assign**.

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To use the User Access and Permissions Assistant:

- API Enabled AND Assign Permission Sets AND Customize Application AND Manage Custom Permissions AND Manage Profiles and Permission Sets AND Manage Session Permission Set Activations AND View Roles and Role Hierarchy AND View Setup and Configuration

EDITIONS

Available in: all editions except **Starter**

USER PERMISSIONS

To use the User Access and Permissions Assistant:

- API Enabled AND Assign Permission Sets AND Customize Application AND Manage Custom Permissions AND Manage Profiles and Permission Sets AND Manage Session Permission Set Activations AND View Roles and Role Hierarchy AND View Setup and Configuration

User Access and Permissions Assistant Considerations

Be aware of these considerations and special behaviors for the User Access and Permissions Assistant.

Accessing the User Access and Permissions Assistant

Verify that the user for the app has been assigned these permission sets.

- User Access & Permissions Assistant Access
- The permission set created during installation to access the Tooling API Credential
- If necessary, any additional permission sets created with the required permissions

Analyzer

When you analyze by user, you must refresh the User Access and Permissions Assistant app each time you want to analyze permissions on a subsequent user.

To refresh the Analyzer feature, select another function, such as Converter or Report, and then return to Permissions Analyzer. Alternately, you can refresh your browser tab.

If you have more than 5,000 users, you can experience slowness and the user that you want to select may not display in the user list.

Converting Profiles to Permission Sets

When converting a profile to a permission set, a variety of factors can cause some records to fail to convert.

- If permissions are associated with deactivated or deprecated features, or bad data, it's possible that the permissions don't convert.
- If Apex classes are running at the time of conversion, it's possible that Setup Entity Access permissions don't convert.

The User Access and Permissions Assistant only supports converting profiles with a Salesforce license.

SEE ALSO:

[Analyze Your Permission Assignments](#)

[Converting Profiles to Permission Sets](#)

[Manage Permission Set Groups](#)

User Access Policies (Beta)

With user access policies, you define aggregated access for your users in a single operation. Automate your users' assignments to permission set licenses, permission sets, permission set groups, package licenses, queues, and groups. You can create policies that grant or remove access whenever users are created or updated, or in a one-time manual migration.

 **Note:** This feature is a Beta Service. Customer may opt to try such Beta Service in its sole discretion. Any use of the Beta Service is subject to the applicable Beta Services Terms provided at [Agreements and Terms](#).

Manual User Access Policies

By default, a user access policy is a one-time process to grant or revoke bulk access for designated users. Use this option to run a single update on a group of selected users. For large groups of users, you can run the user access policy as an asynchronous process.

EDITIONS

Available in: all editions except **Starter**

EDITIONS

Available in: both Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: **Enterprise** and **Unlimited** editions

For example, you're migrating permissions for a group of users from a profile to permission sets and permission set groups. Create filters to identify the users assigned to the profile. Then create actions in the user access policy to add access to the appropriate permission sets and permission set groups.

Active User Access Policies

Use an active user access policy to automatically grant or revoke user access. An active user access policy automatically runs off a triggered event, such as a created or updated user record.

For example, you want to automate the assignment of multiple access mechanisms for Sales Reps in your org. You create a user access policy and set the trigger type to "Create and Update" so that it targets both new users and existing users whose role has changed. You create a filter to identify users who have the Sales Rep role. Then you create actions to grant these users the permission set licenses, permission sets, and permission set groups that they require to do their everyday tasks.

On the detail page for each user access policy, you can see recent user access changes applied by the policy.

[Manually Grant or Revoke Access with a User Access Policy \(Beta\)](#)

Migrate or change users' assignments to access mechanisms with a one-time, manual application of a user access policy.

[Automatically Grant or Revoke Access with a User Access Policy \(Beta\)](#)

Grant or revoke access for a specified set of users through a triggered event, such as a created or updated user record.

[User Access Policy Considerations \(Beta\)](#)

Be aware of these considerations and special behaviors for user access policies.

Manually Grant or Revoke Access with a User Access Policy (Beta)

Migrate or change users' assignments to access mechanisms with a one-time, manual application of a user access policy.

 **Note:** This feature is a Beta Service. Customer may opt to try such Beta Service in its sole discretion. Any use of the Beta Service is subject to the applicable Beta Services Terms provided at [Agreements and Terms](#).

These instructions describe how to create user access policies that you run manually, such as for a user access migration or a one-time user access update. If you want to create user access policies that automatically run whenever qualified user records are created or updated, see [Automatically Grant or Revoke Access with a User Access Policy \(Beta\)](#).

1. From Setup, in the Quick Find box, enter *User Management Settings*, and then select **User Management Settings**. Make sure that both the User Access Policies (Beta) and Enhanced Interface for User Access Policies (Beta) settings are enabled.
If Salesforce enabled user access policies for you before the Summer '23 release, you must enable this feature again on the User Management Settings page.
2. In the Quick Find box, enter *User Access Policies*, and then select **User Access Policies**.
3. Click **New User Access Policy**.
4. Enter a value for the Policy Name and Description. The API Name auto-populates.
5. Click **Save**.
6. On the user access policy's detail page, click **Edit Criteria** to configure the policy's user criteria filters and actions.

EDITIONS

Available in: both Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: **Enterprise** and **Unlimited** editions

USER PERMISSIONS

To modify user access policies:

- [Manage User Access Policies](#)

7. Under Define User Criteria, add at least one user criteria filter. Policies are applied to users that meet all of the criteria filters. You can have:
 - a. Up to three filters for applicable users
 - b. Any number of filters on standard and custom user fields of type Checkbox, Number, Picklist, or Text
 - c. Multiple roles or profiles referenced in the same filter using the `IN` operator
8. Under Define Actions, select **Grant** or **Revoke** from the Action picklist, then select the access mechanism that the action applies to. Access options are:
 - a. Permission sets
 - b. Permission set groups
 - c. Permission set licenses
 - d. Package licenses
 - e. Groups
 - f. Queues

User access policies support up to 20 actions.
9. Save your changes.
10. Click **Apply Policy**. You can select a subset of users to apply the policy to, or click **Apply to All**.

To confirm that the users were granted access correctly, review their individual user records. On the policy's detail page under Recent User Access Changes, you can see when this policy was applied and the affected users.

SEE ALSO:

[User Access Policies \(Beta\)](#)

[Automatically Grant or Revoke Access with a User Access Policy \(Beta\)](#)

[User Access Policy Considerations \(Beta\)](#)

Automatically Grant or Revoke Access with a User Access Policy (Beta)

Grant or revoke access for a specified set of users through a triggered event, such as a created or updated user record.

 **Note:** This feature is a Beta Service. Customer may opt to try such Beta Service in its sole discretion. Any use of the Beta Service is subject to the applicable Beta Services Terms provided at [Agreements and Terms](#).

These instructions describe how to create user access policies that automatically run whenever qualified user records are created or updated. If you want to create user access policies that you run manually, such as for a user access migration or a one-time user access update, see [Manually Grant or Revoke Access with a User Access Policy \(Beta\)](#).

1. From Setup, in the Quick Find box, enter *User Management Settings*, and then select **User Management Settings**. Make sure that both the User Access Policies (Beta) and Enhanced Interface for User Access Policies (Beta) settings are enabled.

If Salesforce enabled user access policies for you before the Summer '23 release, you must enable this feature again on the User Management Settings page.

EDITIONS

Available in: both Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: **Enterprise** and **Unlimited** editions

USER PERMISSIONS

To modify user access policies:

- [Manage User Access Policies](#)

2. In the Quick Find box, enter *User Access Policies*, and then select **User Access Policies**.
3. Click **New User Access Policy**.
4. Enter a value for the Policy Name and Description. The API Name auto-populates.
5. Click **Save**.
6. On the user access policy's detail page, click **Edit Criteria** to configure the policy's user criteria filters and actions.
7. Under Define User Criteria, add at least one user criteria filter. Policies are applied to users that meet all of the criteria filters. You can have:
 - a. Up to three filters for applicable users
 - b. Any number of filters on standard and custom user fields of type Checkbox, Number, Picklist, or Text
 - c. Multiple roles or profiles referenced in the same filter using the **IN** operator
8. Under Define Actions, select **Grant** or **Revoke** from the Action picklist, then select the access mechanism that the action applies to. Access options are:
 - a. Permission sets
 - b. Permission set groups
 - c. Permission set licenses
 - d. Package licenses
 - e. Groups
 - f. QueuesUser access policies support up to 20 actions.
9. Save your changes.
10. Click **Automate Policy**, then select when to trigger the policy:
 - The user access policy runs only when a user who matches the policy criteria is created.
 - The user access policy runs only when a user who matches the policy criteria is updated.
 - The user access policy runs when a user who matches the policy criteria is either created or updated.

11. Click **Activate**.

After you automate the policy, the status changes to Active.

On the policy's detail page under the Recent User Access Changes tab, you can monitor when this policy is applied and the affected users.

SEE ALSO:

[User Access Policies \(Beta\)](#)

[Manually Grant or Revoke Access with a User Access Policy \(Beta\)](#)

[User Access Policy Considerations \(Beta\)](#)

User Access Policy Considerations (Beta)

Be aware of these considerations and special behaviors for user access policies.

-  **Note:** This feature is a Beta Service. Customer may opt to try such Beta Service in its sole discretion. Any use of the Beta Service is subject to the applicable Beta Services Terms provided at [Agreements and Terms](#).

General

An action performed by a user access policy can't trigger another user access policy.

If you revoke access to permission set licenses or managed package licenses, the number of used licenses displayed on the Company Information or Installed Packages Setup pages doesn't always reflect these updates.

The Recent User Access Changes section shows only changes applied by the policy that are still in effect. If access changes applied by a policy are later overridden, either by another user access policy or a manual operation, those changes are no longer displayed under Recent User Access Changes.

Active Policies

You can have up to 20 active user access policies at a time.

If a user record creation or update triggers more than one user access policy, the most recently modified user access policy that matches the criteria is applied.

SEE ALSO:

- [User Access Policies \(Beta\)](#)
- [Manually Grant or Revoke Access with a User Access Policy \(Beta\)](#)
- [Automatically Grant or Revoke Access with a User Access Policy \(Beta\)](#)

Profiles

Profiles define default settings for users. When you create users, you assign a profile to each one.

Watch the video to see how you can configure profiles.

 [Watch a video](#)

Your org includes several standard profiles where you can edit a limited number of settings. With editions that contain custom profiles, you can edit all permissions and settings except the user license. In Contact Manager and Group Edition orgs, you can assign standard profiles to your users, but you can't view or edit the standard profiles, and you can't create custom profiles.

Every profile belongs to exactly one user license type.

-  **Note:** When possible, assign users the Minimum Access - Salesforce profile, and then use permission sets and permission set groups to grant users only the permissions that they require. Apply permission sets to users based on the tasks that they do rather than their job title. Because you can reuse smaller permission set building blocks, you can avoid creating dozens or even hundreds of profiles for each user and job function. For more information, see [Permission Sets](#) in Salesforce Help.

EDITIONS

Available in: both Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: **Enterprise** and **Unlimited** editions

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

Custom Profiles available in: **Essentials, Professional, Enterprise, Performance, Unlimited**, and **Developer** Editions

Standard Profiles

Every Salesforce org includes standard profiles that you can assign to users. Edits to standard profiles are limited to certain settings.

Create and Edit Profile List Views

If enhanced profile list views are enabled for your organization, you can create profile list views to view a set of profiles with the fields that you choose. For example, you can create a list view of all profiles with Modify All Data enabled.

Edit Multiple Profiles with Profile List Views

If enhanced profile list views are enabled for your organization, you can change permissions in up to 200 profiles directly from the list view, without accessing individual profile pages.

Create or Clone Profiles

Create custom profiles using the API, or clone existing profiles and customize them to fit your business's needs.

View a Profile's Assigned Users

View and manage all users assigned to a profile from the profile's overview page.

Configure Default Settings in Profiles

Configure assigned apps, record types, page layouts, and other default settings in profiles so that assigned users can see the data and apps required to complete their work.

Search in the Enhanced Profile User Interface

To locate an object, tab, permission, or setting name on a profile page, type at least three consecutive letters in the Find Settings... box. As you type, suggestions for results that match your search terms appear in a list. Click an item in the list to go to its settings page.

Standard Profiles

Every Salesforce org includes standard profiles that you can assign to users. Edits to standard profiles are limited to certain settings.

Every org includes standard profiles. In Professional, Enterprise, Unlimited, Performance, and Developer Editions, you can use standard profiles or create, edit, and delete custom profiles. In orgs where you can't create custom profiles, such as Contact Manager and Group Editions, you can assign standard profiles to your users, but you can't view or edit them.

While you can't edit standard profile permissions, you can edit the following settings:

- Custom App Settings
- Tab Settings
- Desktop Integration Clients options
- Session Settings
- Password Policies

The following table lists commonly used permissions in standard profiles.

Profile Name	Available Permissions
System Administrator	Can configure and customize the application. Has access to all functionality that doesn't require an extra license. For example, administrators can't manage campaigns unless they also have a Marketing User license. Can manage price books and products.
Standard Platform User	Can use custom AppExchange apps developed in your org or installed from AppExchange. In addition, can use core platform

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Your edition determines which standard profiles are available.

Profile Name	Available Permissions
	functionality such as accounts, contacts, reports, dashboards, and custom tabs.
Standard Platform One App User	Can use one custom AppExchange app developed in your org or installed from AppExchange. The custom app is limited to five tabs. In addition, can use core platform functionality such as accounts, contacts, reports, dashboards, and custom tabs.
Standard User	Can create and edit most major types of records, run reports, and view the org's setup. Can view, but not manage, campaigns. Can create, but not review, solutions.
Minimum Access - API Only Integrations	Grants access to Salesforce only through the API. Assign more permissions to a user through permission sets. Replaces the deprecated Salesforce API Only System Integrations user profile, which isn't available in newly provisioned orgs. For more information about using this profile for integration users, see Give Integration Users API Only Access .
Customer Community User	Can log in via an Experience Cloud site. Your site settings and sharing model determine their access to tabs, objects, and other features. For more information, see Experience Cloud User Licenses .
Customer Community Plus User	
Partner Community User	
Partner User	Can log in via a partner portal or an Experience Cloud site.
Solution Manager	Can review and publish solutions. Also has access to the same functionality as the Standard User.
Marketing User	Can manage campaigns, create letterheads, create HTML email templates, manage public documents, and add campaign members and update their statuses with the Data Import Wizard. Also has access to the same functionality as the Standard User.
Contract Manager	Can create, edit, activate, and approve contracts. This profile can also delete contracts as long as they aren't activated.
Read Only	<p> Note: The Read Only standard profile was converted to a custom profile in existing Salesforce orgs with the rollout of the Summer '21 release. This change allows you to edit permissions and rename the profile. New orgs created in Spring '21 and later don't have the Read Only standard profile, but these orgs can use the Minimum Access profile and assign custom permission sets to grant users read access as required. For more information, see the knowledge article, Read Only Profile Conversion to Custom Profile.</p> <p>Can view the org's setup, run and export reports, and view, but not edit, other records.</p>

Profile Name**Available Permissions**

Chatter Moderator User

Can log in to Chatter. Can access all standard Chatter people, profiles, groups, and files. This user can also:

- Activate and deactivate other Chatter Free users and moderators
- Grant and revoke moderator privileges
- Delete posts and comments that they can see
- Edit their own posts and comments

 **Note:** Changing a user's profile from Chatter Moderator User to Chatter Free User removes moderator privileges in Chatter.

Minimum Access - Salesforce

Grants the least privileges in the Salesforce platform. It includes Access Activities, Chatter Internal User, Lightning Console User, and View Help Link permissions. Follow data security best practices to assign this profile, and then add more permissions for the user through permission sets and permission set groups.

Site.com Only User

Can only log in to the Site.com app. Each Site.com Only user also needs a Site.com Publisher feature license to create and publish sites, or a Site.com Contributor feature license to edit the site's content.

This user can also:

- Use one custom app with up to 20 custom objects
- Access the Content app, but not the Accounts and Contacts objects
- Create unlimited custom tabs

Only available with the Site.com Only user license.

SEE ALSO:[Profiles](#)[User Permissions](#)

Create and Edit Profile List Views

If enhanced profile list views are enabled for your organization, you can create profile list views to view a set of profiles with the fields that you choose. For example, you can create a list view of all profiles with Modify All Data enabled.

 **Note:** If Profile Filtering is enabled in your org, users need permissions to view the profile names of other users.

1. From Setup, in the Quick Find box, enter *Profiles*, and then select **Profiles**.
2. In the Profiles page, click **Create New View**, or select a view and click **Edit**.
3. Enter the view name.
4. Under Specify Filter Criteria, specify the conditions that the list items must match, such as *Modify All Data equals True*.
 - a. To search for and select the setting you want, type a setting name, or click the lookup icon.
 - b. Choose a filter operator.
 - c. Enter the value that you want to match.
 - d. To specify another filter condition, click **Add New**. You can specify up to 25 filter condition rows.

To remove a filter condition row and clear its values, click the remove row icon.

5. Under Select Columns to Display, specify the profile settings that you want to appear as columns in the list view. You can add up to 15 columns in a single list view.
 - a. From the Search dropdown list, select the type of setting you want to search for.
 - b. Enter part or all of a word in the setting you want to add and click **Find**.

 **Note:** If the search finds more than 500 values, no results appear. Use the preceding steps to refine your search criteria and show fewer results.

- c. To add or remove columns, select one or more column names and click the **Add** or **Remove** arrow.
 - d. Use the **Top**, **Up**, **Down**, and **Bottom** arrows to arrange the columns in the sequence you want.
6. Click **Save**, or if you're cloning an existing view, rename it and click **Save As**.

SEE ALSO:

[Edit Multiple Profiles with Profile List Views](#)

[Limit Profile Details to Required Users](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

Custom Profiles available in: **Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To create, edit, and delete profile list views:

- Manage Profiles and Permission Sets

Edit Multiple Profiles with Profile List Views

If enhanced profile list views are enabled for your organization, you can change permissions in up to 200 profiles directly from the list view, without accessing individual profile pages.

Editable cells display a pencil icon (✎) when you hover over the cell, while non-editable cells display a lock icon (🔒). In some cases, such as in standard profiles, the pencil icon appears but the setting isn't actually editable.

 **Warning:** Use care when editing profiles with this method. Because profiles affect a user's fundamental access, making mass changes may have a widespread effect on users in your organization.

1. Select or [create](#) a list view that includes the profiles and permissions you want to edit.
2. To edit multiple profiles, select the checkbox next to each profile you want to edit.
If you select profiles on multiple pages, Salesforce remembers which profiles are selected.

3. Double-click the permission you want to edit.
For multiple profiles, double-click the permission in any of the selected profiles.

4. In the dialog box that appears, enable or disable the permission.
In some cases, changing a permission may also change other permissions. For example, if "Customize Application" and "View Setup and Configuration" are disabled and you enable "Customize Application," then "View Setup and Configuration" is also enabled. In this case, the dialog box lists the affected permissions.

5. To change multiple profiles, select **All n selected records** (where n is the number of profiles you selected).
6. Click **Save**.

 **Note:**

- For standard profiles, inline editing is available only for the "Single Sign-On" and "Affected By Divisions" permissions.
- If you edit multiple profiles, only those profiles that support the permission you're changing will change. For example, if you use inline editing to add "Modify All Data" to multiple profiles, but because of its user license the profile doesn't have "Modify All Data," the profile won't change.

If any errors occur, an error message appears, listing each profile in error and a description of the error. Click the profile name to open the profile detail page. The profiles you've clicked appear in the error window in gray, strike-through text. To view the error console, you must have pop-up blockers disabled for the Salesforce domain.

Any changes you make are recorded in the setup audit trail.

SEE ALSO:

[Profiles](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To edit multiple profiles from the list view:

- Manage Profiles and Permission Sets
- AND
- Customize Application

Create or Clone Profiles

Create custom profiles using the API, or clone existing profiles and customize them to fit your business's needs.

-  **Tip:** If you clone profiles to enable certain permissions or access settings, consider using permission sets. Because you can reuse smaller permission set building blocks, you can avoid creating dozens or even hundreds of profiles for each user and job function.

To create an empty custom profile without any base permissions included, use the Profile SOAP API object. On the Profile Setup page, you must first clone an existing profile to create a custom profile.

1. To clone a profile, from Setup, in the Quick Find box, enter *Profiles*, and then select **Profiles**.
2. In the Profiles list page, do one of the following:
 - Click **New Profile**, then select an existing profile that's similar to the one you want to create.
 - If enhanced profile list views are enabled, click **Clone** next to a profile that's similar to the one you want to create.
 - Click the name of a profile that's similar to the one you want to create, then in the profile page, click **Clone**.

A new profile uses the same [user license](#) as the profile it was cloned from.

3. Enter a profile name.
4. Click **Save**.

SEE ALSO:

[SOAP API Developer Guide: Profile Profiles](#)
[Permission Sets](#)

View a Profile's Assigned Users

View and manage all users assigned to a profile from the profile's overview page.

1. From Setup, in the Quick Find box, enter *Profiles*, and then click **Profiles**.
2. Select a profile.
3. Depending on which user interface you're using, do one of the following.
 - In the enhanced profile user interface, click **Assigned Users**.
 - In the original profile user interface, click **View Users**.

SEE ALSO:

[Profiles](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

Custom Profiles available in: **Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To create profiles:

- [Manage Profiles and Permission Sets](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

Custom Profiles available in: **Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Configure Default Settings in Profiles

Configure assigned apps, record types, page layouts, and other default settings in profiles so that assigned users can see the data and apps required to complete their work.

Profiles are one of the features that determine what users can see and do. For each profile, we recommend that you configure the following:

- [Assigned apps](#)
- [Record types and page layouts](#)
- [Login hours](#)
- [Login IP ranges](#)
- [Password policies](#)
- [Session settings](#)

You can also configure user, object, and field permissions in profiles. However, we strongly recommend that you use permission sets and permission set groups to manage your users' permissions. Because you can reuse smaller permission set building blocks, you can avoid creating dozens or even hundreds of profiles for each user and job function. For more information, see [Permissions Sets](#) in Salesforce Help.

Depending on your Salesforce org, settings for other features and apps are available to configure in profiles.

SEE ALSO:

[Enable Enhanced Profile List Views](#)

[Enable the Enhanced Profile User Interface](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

Custom Profiles available in: **Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To view profiles:

- [View Setup and Configuration](#)

To delete profiles and edit profile properties:

- [Manage Profiles and Permission Sets](#)

View and Edit Assigned Apps in Profiles

Assigned app settings specify the apps that users can select in the Lightning Platform app menu.

Every profile must have at least one visible app, except profiles associated with Customer Portal users because apps aren't available to them.

To specify app visibility:

1. From Setup, in the Quick Find box, enter *Profiles*, and then select **Profiles**.
2. Select a profile.
3. Depending on which user interface you're using, do one of the following:
 - In the enhanced profile user interface, click **Assigned Apps**, and then click **Edit**.
 - In the original profile user interface, click **Edit**, and then scroll to the Custom App Settings section.
4. Select one default app. The default app appears when users log in for the first time.
5. Select **Visible** for any other apps that you want to make visible.

SEE ALSO:

[Configure Default Settings in Profiles Profiles](#)

Assign Record Types and Page Layouts in Profiles

Configure the record type and page layout assignment mappings that are used when users view records.

The steps for configuring record types and page layouts depend on whether you're using the enhanced profile user interface or the original profile user interface.

[Assign Record Types and Page Layouts in the Enhanced Profile User Interface](#)

In the enhanced profile user interface, you can configure record type and page layout settings in each individual object's settings.

[Assign Record Types to Profiles in the Original Profile User Interface](#)

After you create record types and include picklist values in them, add record types to user profiles.

[Assign Page Layouts in the Original Profile User Interface](#)

In the original profile user interface, you can access, view, and edit all page layout assignments easily in one location.

Assign Record Types and Page Layouts in the Enhanced Profile User Interface

In the enhanced profile user interface, you can configure record type and page layout settings in each individual object's settings.

1. From Setup, in the Quick Find box, enter *Profiles*, and then select **Profiles**.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

Custom Profiles available in: **Essentials, Professional, Enterprise, Performance, Unlimited**, and **Developer** Editions

USER PERMISSIONS

To edit app visibility settings:

- [Manage Profiles and Permission Sets](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited**, and **Developer** Editions

Record types available in: **Professional, Enterprise, Performance, Unlimited**, and **Developer** Editions

USER PERMISSIONS

To assign record types and page layouts in profiles:

- [Manage Profiles and Permission Sets](#)

2. Select a profile.
3. In the Find Settings... box, enter the name of the object you want, select it, and then click **Edit**.
4. In the Record Types and Page Layout Assignments section, make changes to the settings as needed.
 - **Record Types:** Lists all existing record types for the object.
 - Master-- is a system-generated record type that's used when a record has no custom record type associated with it. When --Master-- is assigned, users can't set a record type to a record, such as during record creation. All other record types are custom record types.
 - **Page Layout Assignment:** The page layout to use for each record type. The page layout determines the buttons, fields, related lists, and other elements that users with this profile see when creating records with the associated record type. Since all users can access all record types, every record type must have a page layout assignment, even if the record type isn't specified as an assigned record type in the profile.
 - **Assigned Record Types:** Record types that are checked in this column are available when users with this profile create records for the object. If --Master-- is selected, you can't select any custom record types; and if any custom record types are selected, you can't select --Master--.
 - **Default Record Type:** The default record type to use when users with this profile create records for the object.

The Record Types and Page Layout Assignments settings have some variations for the following objects or tabs.

Object or Tab	Variation
Accounts	If your organization uses person accounts, the accounts object additionally includes Business Account Default Record Type and Person Account Default Record Type settings, which specify the default record type to use when the profile's users create business or person account records from converted leads.
Cases	The cases object additionally includes Case Close settings, which show the page layout assignments to use for each record type on closed cases. That is, the same record type may have different page layouts for open and closed cases. With this additional setting, when users close a case, the case may have a different page layout that exposes how it was closed.
Home	You can't specify custom record types for the home tab. You can only select a page layout assignment for the --Master-- record type.

5. Click **Save**.

Assign Record Types to Profiles in the Original Profile User Interface

After you create record types and include picklist values in them, add record types to user profiles.

 **Note:** Users can view records of any record type, even if the record type isn't associated with their profile.

You can associate several record types with a profile. For example, a user needs to create hardware and software sales opportunities. In this case, you can create and add both "Hardware" and "Software" record types to the user's profile.

1. From Setup, in the Quick Find box, enter *Profiles*, and then select **Profiles**.
2. Select a profile. The record types available for that profile are listed in the Record Type Settings section.
3. Click **Edit** next to the appropriate type of record.

4. Select a record type from the Available Record Types list and add it to the Selected Record Types list.

Master is a system-generated record type that's used when a record has no custom record type associated with it. When you assign **Master**, users can't set a record type to a record, such as during record creation. All other record types are custom record types.

5. From **Default**, choose a default record type.

If your organization uses person accounts, this setting also controls which account fields display in the **Quick Create** area of the accounts home page.

6. If your organization uses person accounts, set default record type options for both person accounts and business accounts. From the **Business Account Default Record Type** and then the **Person Account Default Record Type** drop-down list, choose a default record type.

These settings are used when defaults are needed for both kinds of accounts, such as when converting leads.

7. Click **Save**.

Options in the Record Type Settings section are blank wherever no record types exist. For example, if you have two record types for opportunities but no record types for accounts, the **Edit** link only displays for opportunities. In this example, the picklist values and default value for the master are available in all accounts.

-  **Note:** If your organization uses person accounts, you can view the record type defaults for business accounts and person accounts. Go to Account Record Type Settings in the profile detail page. Clicking **Edit** in the Account Record Type Settings is another way to begin setting record type defaults for accounts.

Assign Page Layouts in the Original Profile User Interface

In the original profile user interface, you can access, view, and edit all page layout assignments easily in one location.

1. From Setup, in the Quick Find box, enter *Profiles*, and then select **Profiles**.
2. Select a profile.
3. Click **View Assignment** next to any tab name in the Page Layouts section.
4. Click **Edit Assignment**.
5. Use the table to specify the page layout for each profile. If your organization uses record types, a matrix displays a page layout selector for each profile and record type.
Selected page layout assignments are highlighted. Page layout assignments you change are italicized until you save your changes.
6. If necessary, select another page layout from the **Page Layout To Use** drop-down list and repeat the previous step for the new page layout.
7. Click **Save**.

SEE ALSO:

[How Is Record Type Access Specified?](#)

[Assign Custom Record Types in Permission Sets](#)

[Configure Default Settings in Profiles](#)

View and Edit Login Hours in Profiles

Specify the hours when users can log in based on the user profile.

1. From Setup, in the Quick Find box, enter *Profiles*, and then select **Profiles**.
2. Select a profile.
3. Depending on which user interface you're using, do one of the following:
 - In the enhanced profile user interface, click **Login Hours**, and then click **Edit**.
 - In the original profile user interface, scroll down to the Login Hours related list, and then click **Edit**.
4. Set the days and hours when users with this profile can log in to the org.

To let users log in at any time, click **Clear all times**. To prohibit users from logging in on a specific day, set Start Time to **12 AM** and End Time to **12 AM**.

If users are logged in when their login hours end, they can continue to view their current page, but they can't take any further action.

5. Click **Save**.

 **Note:** The first time login hours are set for a profile, the hours are based on the org's default time zone as specified on the Company Information page in Setup. After that, changes to the org's default time zone on the Company Information page don't affect the time zone for the profile's login hours. The profile login hours remain the same, even when a user is in a different time zone or the org's default time zone changes.

Depending on whether you're viewing or editing login hours, the hours appear differently. On the profile detail page, hours appear in your specified time zone. On the Login Hours edit page, the hours appear in the org's default time zone.

SEE ALSO:

- [Restrict Login IP Addresses in Profiles](#)
- [Configure Default Settings in Profiles](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To set login hours:

- [Manage Profiles and Permission Sets](#)

Restrict Login IP Addresses in Profiles

Control login access at the user level by specifying a range of allowed IP addresses on a user's profile. When you define IP address restrictions for a profile, a login from any other IP address is denied.

How you restrict the range of valid IP addresses on a profile depends on your Salesforce edition.

- If you're using an Enterprise, Unlimited, Performance, or Developer Edition, manage valid IP addresses in profiles.
- If you're using a Group, or Personal Edition, from Setup, manage valid IP addresses on the Session Settings page.
- In a Professional Edition, the location of IP ranges depends on whether you have the "Edit Profiles & Page Layouts" org preference enabled as an add-on feature. With the "Edit Profiles & Page Layouts" org preference enabled, IP ranges are on individual profiles. Without the "Edit Profiles & Page Layouts" org preference enabled, IP ranges are on the Session Settings page.

To restrict IP addresses in profiles:

1. From Setup, in the Quick Find box, enter *Profiles*, and then select **Profiles**.
2. Depending on which user interface you're using, do one of the following:
 - In the enhanced profile user interface, click **Login IP Ranges**, and then click **Add IP ranges**.
 - In the original profile user interface, scroll down to the Login IP Ranges related list, and then click **New**.
3. Specify allowed IP addresses for the profile. Enter a valid IP address in the `IP Start Address` field and a higher-numbered IP address in the `IP End Address` field. To allow logins from a single IP address, enter the same address in both fields.

The IP addresses in a range must be either IPv4 or IPv6. In ranges, IPv4 addresses exist in the IPv4-mapped IPv6 address space `::ffff:0:0 to ::ffff:ffff:ffff`, where `::ffff:0:0` is `0.0.0.0` and `::ffff:ffff:ffff` is `255.255.255.255`. A range can't include IP addresses both inside and outside of the IPv4-mapped IPv6 address space. Ranges like `255.255.255.255 to ::1:0:0:0` or `:: to ::1:0:0:0` aren't allowed.

 **Note:** Partner User profiles are limited to five IP addresses. To increase this limit, contact Salesforce.
4. Optionally enter a description for the range. If you maintain multiple ranges, use the Description field to provide details, such as which part of your network corresponds to this range.
5. Click **Save**.

You can further restrict access to Salesforce to only those IPs in Login IP Ranges. To enable this option, in Setup, in the Quick Find box, enter *Session Settings*, and then select **Session Settings**. Select **Enforce login IP ranges on every request**. This option affects all user profiles that have login IP restrictions.

-  **Note:** Cache settings on static resources are set to private when accessed via a Salesforce Site whose guest user's profile has restrictions based on IP range or login hours. Sites with guest user profile restrictions cache static resources only within the browser. Also, if a previously unrestricted site becomes restricted, it can take up to 45 days for the static resources to expire from the Salesforce cache and any intermediate caches.

SEE ALSO:

- [Set Trusted IP Ranges for Your Organization](#)
- [View and Edit Login Hours in Profiles](#)
- [Configure Default Settings in Profiles](#)

EDITIONS

Available in: Salesforce Classic (**not available in all orgs**) and Lightning Experience

Available in: **All Editions**

USER PERMISSIONS

To view login IP ranges:

- View Setup and Configuration

To edit and delete login IP ranges:

- Manage Profiles and Permission Sets

View and Edit Password Policies in Profiles

To ensure that the appropriate level of password security is used for your organization, specify password requirements with Password Policies settings for users assigned to a profile. Profile Password Policies settings override the organization-wide Password Policies for that profile's users. If you don't set Password Policies on a profile, the organization-wide Password Policies apply. New profile Password Policies take effect for existing profile users when they reset their passwords.

Changes to the organization-wide Password Policies don't apply to users of a profile with its own Password Policies.

1. From Setup, in the Quick Find box, enter *Profiles*, and then select **Profiles**.
2. Select a profile.
3. Depending on which user interface you're using, do one of the following.
 - In the enhanced profile user interface, click **Password Policies**, then click **Edit**.
 - In the original profile user interface, click **Edit**, then scroll to the Password Policies section.
4. Change the values for the profile.

 **Note:** You can change this setting to an expiration date that is earlier or later than the previous expiration date. To remove an expiration date, select **Never expires**.
5. Click **Save**.

Password Policy Fields in Profiles

Specify password requirements with Password Policies settings. Understand how each field impacts a profile's password requirements.

Password Policy Fields in Profiles

Specify password requirements with Password Policies settings. Understand how each field impacts a profile's password requirements.

Changes to org-wide password policies don't apply to users of a profile that has its own password policies.

Field	Description
User passwords expire in	<p>The length of time until a user password expires and must be changed. The default is 90 days. This setting isn't available for Self-Service portals. Enabling the Password never expires policy overrides the User passwords expire in policy.</p> <p>You can change this setting to an expiration date that is earlier or later than the previous expiration date. To remove an expiration date, select Never expires.</p>
Enforce password history	<p>Save users' previous passwords so that they must use a new, unique password when changing passwords. Password history isn't saved until you set this value. The default is 3 passwords remembered. You can't select No passwords remembered unless you select Never expires for the</p>

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

Custom Profiles available in: **Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To edit session and password settings in profiles:

- Manage Profiles and Permission Sets

To set password policies:

- Manage Password Policies

Field	Description
Minimum password length	<p data-bbox="818 258 1446 323">User passwords expire in field. This setting isn't available for Self-Service portals.</p> <p data-bbox="818 348 1446 443">The minimum number of characters required for a password. When you set this value, existing users aren't affected until the next time they change their passwords. The default is 8 characters.</p>
Password complexity requirement	<p data-bbox="818 474 1446 501">The types of characters that must be used in a user's password.</p> <ul data-bbox="818 520 1446 1457" style="list-style-type: none"> <li data-bbox="818 520 1446 585">• No restriction—Has no requirements and is the least secure option. <li data-bbox="818 596 1446 695">• Must include alpha and numeric characters—The default setting. Requires at least one alphabetic character and one number. <li data-bbox="818 705 1446 877">• Must include alpha, numeric, and special characters—Requires at least one alphabetic character, one number, and one of the following characters: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~. <li data-bbox="818 888 1446 987">• Must include numbers and uppercase and lowercase letters—Requires at least one number, one uppercase letter, and one lowercase letter. <li data-bbox="818 997 1446 1201">• Must include numbers, uppercase and lowercase letters, and special characters—Requires at least one number, one uppercase letter, one lowercase letter, and one of the following characters: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~. <li data-bbox="818 1211 1446 1457">• Must include 3 of the following: numbers, uppercase letters, lowercase letters, special characters—Requires at least three of the following options: one number, one uppercase letter, one lowercase letter, and one special character (! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~). <p data-bbox="818 1476 1446 1535">Only the characters listed meet the requirement. Other symbol characters aren't considered special characters.</p>
Password question requirement	<p data-bbox="818 1577 1446 1642">The restrictions to place on the password hint's answer. This setting isn't available for Self-Service portals.</p>
Maximum invalid login attempts	<p data-bbox="818 1665 1446 1730">The number of login failures allowed for a user before the user is locked out. This setting isn't available for Self-Service portals.</p>
Lockout effective period	<p data-bbox="818 1753 1446 1818">The duration of the login lockout. The default is 15 minutes. This setting isn't available for Self-Service portals.</p> <p data-bbox="818 1829 1446 1900">When a user is logged in to an active session but is later locked out, the user remains logged in to the active session.</p>

Field	Description
Obscure secret answer for password resets	<p>A locked-out user must wait until the lockout period expires. Alternatively, a user with the Reset User Passwords and Unlock Users permission can unlock a user from the Users detail page in Setup.</p> <p>Hide answers to security questions as the user types. The default is to show the answer in plain text.</p> <p>If your org uses the Microsoft Input Method Editor (IME) with the input mode set to Hiragana, when you type ASCII characters, they're converted in to Japanese characters in normal text fields. However, the IME doesn't work properly in fields with obscured text. If your org's users can't properly enter their passwords or other values after enabling this feature, disable the feature.</p>
Require a minimum 1 day password lifetime	<p>A password can't be changed more than once in a 24-hour period. This policy applies to all password changes, including password resets by Salesforce admins.</p>
Don't immediately expire links in forgot password emails	<p>When you select this option, a password reset link in a forgot password email doesn't expire the first time it's clicked. Instead, the link stays active until the user confirms the password reset request on an interstitial page.</p> <p>A user has 24 hours to reset a password. After 24 hours, the user must submit another request.</p>

SEE ALSO:

[View and Edit Password Policies in Profiles](#)

Edit Session Settings in Profiles

You can control session settings on a user profile basis. If you don't configure the profile session settings, the org's session settings apply to users of the profile. When set, the profile settings override the org-wide settings.

1. From Setup, in the Quick Find box, enter *Profiles*, and then select **Profiles**.
2. Select a profile.
3. Depending on which user interface you're using, take the corresponding step.
 - In the enhanced profile user interface, click **Session Settings**, and then click **Edit**.
 - In the original profile user interface, click **Edit**, and then scroll to the Session Settings section.
4. For Session Times Out After, select a timeout value from the dropdown list.
Set how many minutes or hours of inactivity elapse before a user's authentication session times out. At the end of the session, the user must log in again.
5. For Session Security Level Required at Login, select **High Assurance** to require users to verify their identity with multi-factor authentication when they log in. After users authenticate successfully, they're logged in to Salesforce.

It's possible that users are prompted to verify their identity with multi-factor authentication twice during the OAuth approval flow. The first challenge is on the UI session. The second challenge happens when the access token is bridged into the UI because the High Assurance session security level isn't transferred to the access token.

6. Enable different login policies for your org's employees depending on whether they log in to Salesforce or an Experience Cloud site.
 - a. To give employees less restrictive access to a site as compared to logging in to Salesforce, select **Separate Experience Cloud site and Salesforce login authentication for employees**.

Employees are often required to log in to Salesforce from the corporate network or VPN. If you don't select this option, employees have the same policies for logging in to Salesforce and to their Experience Cloud sites.

When you select this option, Salesforce and Experience Cloud sites are treated as separate apps, so you can loosen site login policies for employees. As a result, employees with an active Salesforce session can be required to log in again when accessing a site. And employees who log in to a site can be required to log in to Salesforce.

When employees who have these options enabled in their profile navigate to Experience Cloud site workspaces, they're prompted to log in to the site again. Users who have these options enabled and the required permissions can still create Experience Cloud sites.



Note: External customers and partners can typically log in to Experience Cloud sites without such restrictive login policies.

- b. To ignore IP address restrictions for this user profile, select **Relax login IP restrictions**.
 - c. To make it easier for Salesforce Customer Support representatives to troubleshoot issues, select **Skip Device Activation at Login**. Enabling this permission allows only a Customer Support rep to skip device activation when they log in to the account. Users with the permission still must verify their identity when they log in from an unrecognized browser, device, or IP address.
 - d. To support authorization with OAuth for employees who have **Separate Experience Cloud site and Salesforce login authentication for employees** enabled on their profile, select **Allow OAuth for employees**.
7. If you're working with a customer or partner's profile, these extra settings appear.

EDITIONS

Available in: both Salesforce Classic (**not available in all orgs**) and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

Custom Profiles available in: **Essentials, Professional, Enterprise, Performance, Unlimited**, and **Developer** Editions

USER PERMISSIONS

To edit session and password settings in profiles:

- Manage Profiles and Permission Sets

- a.  **Note:** This feature is a Beta Service. Customer may opt to try such Beta Service in its sole discretion. Any use of the Beta Service is subject to the applicable Beta Services Terms provided at [Agreements and Terms](#).

To extend customer or partner user sessions to last up to 7 days, for **Session Times Out After** select a timeout value from the dropdown list (beta).

Extend the session length to make it easy for your customers and partners to stay in your Experience Cloud site. This option applies only to the External Identity license, which enables access to the Salesforce Customer Identity product, and the High Volume Customer Portal user license, which enables limited access for users in orgs that have thousands to millions of users.

- b. To prevent customers or partners from being logged out when they close the browser, select **Keep users logged in when they close the browser** (beta).

This setting lets customer or partner user sessions remain active until users log out of the site or when the session times out. If unselected, customers or partners are logged out when they close their browser. This option applies only to the External Identity license, which enables access to the Customer Identity product, and the High Volume Customer Portal user license, which enables limited access for users in orgs that have thousands to millions of users.

- c. To add more security when customers or partners log in, select **Enable device activation for customers**. This option applies to users with community licenses or the External Identity license.

When selected, Salesforce requires customers or partners to verify their identity when they log in from a different browser or device.

- d. To allow employees within your org to bypass device activation when they log in to an Experience Cloud site, select **Skip employee device activation during Experience Cloud site login**.

This setting doesn't allow employees to skip device activation when they log in to your org.

8. Save your changes.

App and System Settings in the Enhanced Profile User Interface

In the enhanced profile user interface, administrators can easily navigate, search, and modify settings for a single profile. Permissions and settings are organized into pages under app and system categories, which reflect the rights users need to administer and use app and system resources.

App Settings

Apps are sets of tabs that users can change by selecting the drop-down menu in the header. All underlying objects, components, data, and configurations remain the same, regardless of the selected app. In selecting an app, users navigate in a set of tabs that allows them to efficiently use the underlying functionality for app-specific tasks. For example, let's say you do most of your work in the sales app, which includes tabs like Accounts and Opportunities. To track a new marketing campaign, rather than adding the Campaigns tab to the sales app, you select Marketing from the app drop-down to view your campaigns and campaign members.

In the enhanced profile user interface, the Apps section of the overview page contains settings that are directly associated with the business processes that the apps enable. For profiles, we recommend that you configure these app settings:

- Assigned apps
- Record types and page layouts (under Object Settings)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

System Settings

Some system functions apply to an organization and not to any single app. For example, login hours and login IP ranges control a user's ability to log in, regardless of which app the user accesses. For profiles, we recommend that you configure these system settings:

- Login hours
- Login IP ranges
- Session settings
- Password policies

 **Note:** You can also configure user, object, and field permissions in profiles under App Settings and System Settings. However, we strongly recommend that you use permission sets and permission set groups to manage your users' permissions. Because you can reuse smaller permission set building blocks, you can avoid creating dozens or even hundreds of profiles for each user and job function. For more information, see [Permissions Sets](#) in Salesforce Help.

SEE ALSO:

[Configure Default Settings in Profiles](#)

[Enable the Enhanced Profile User Interface](#)

Edit Object Permissions in Profiles

Object permissions specify the type of access that users have to objects.

We strongly recommend that you use permission sets and permission set groups instead of profiles to manage your users' object permissions. Because you can reuse smaller permission set building blocks, you can avoid creating dozens or even hundreds of profiles for each user and job function. For more information, see [Permissions Sets](#) in Salesforce Help.

 **Note:** As of Winter '21 and later, editing standard objects on standard profiles is disabled.

1. From Setup, in the Quick Find box, enter *Profiles*, and then select **Profiles**.
2. Select a profile.
3. Depending on which user interface you're using, do one of the following.
 - In the enhanced profile user interface, in the Find Settings... box, enter the name of the object and select it from the list. Click **Edit**, then scroll to the Object Permissions section.
 - In the original profile user interface, click **Edit**, then scroll to the Standard Object Permissions, Custom Object Permissions, or External Object Permissions section.

 **Note:** If your org has more than 500 custom objects and you search for object settings in a profile, they don't load. To see all objects, click **Object Settings**.

4. Specify the object permissions.
5. Click **Save**.

SEE ALSO:

[Object Permissions](#)

[Profiles](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To view object permissions:

- View Setup and Configuration

To edit object permissions:

- Manage Profiles and Permission Sets
- AND
- Customize Application

Enable Custom Permissions in Profiles

Custom permissions give you a way to provide access to custom processes or apps. After you've created a custom permission and associated it with a process or app, you can enable the permission in profiles.

We strongly recommend that you use permission sets and permission set groups instead of profiles to manage your users' custom permissions. Because you can reuse smaller permission set building blocks, you can avoid creating dozens or even hundreds of profiles for each user and job function. For more information, see [Permissions Sets](#) in Salesforce Help.

1. From Setup, in the Quick Find box, enter *Profiles*, and then select **Profiles**.
2. Select a profile.
3. Depending on which user interface you're using, do one of the following.
 - In the enhanced profile user interface, click **Custom Permissions**, and then click **Edit**.
 - In the original profile user interface, in the Enabled Custom Permissions related list, click **Edit**.
4. To enable custom permissions, select them from the Available Custom Permissions list and click **Add**. To remove custom permissions from the profile, select them from the Enabled Custom Permissions list and click **Remove**.
5. Click **Save**.

SEE ALSO:

[Custom Permissions](#)

Search in the Enhanced Profile User Interface

To locate an object, tab, permission, or setting name on a profile page, type at least three consecutive letters in the Find Settings... box. As you type, suggestions for results that match your search terms appear in a list. Click an item in the list to go to its settings page.

Search terms aren't case-sensitive. For some categories, you can search for the specific permission or setting name. For other categories, search for the category name.

Item	Search for	Example
Assigned apps	App name	Type <i>sales</i> in the Find Settings box, then select <i>Sales</i> from the list.
Objects	Object name	Let's say you have an Albums custom object. Type <i>albu</i> , then select <i>Albums</i> .
<ul style="list-style-type: none"> • Fields • Record types • Page layout assignments 	Parent object name	Let's say your Albums object contains a Description field. To find the <i>Description</i> field for albums, type <i>albu</i> , select <i>Albums</i> , and scroll down to <i>Description</i> under Field Permissions.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

In Group and Professional Edition organizations, you can't create or edit custom permissions, but you can install them as part of a managed package.

USER PERMISSIONS

To enable custom permissions in profiles:

- [Manage Profiles and Permission Sets](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

The available profile permissions and settings vary according to which Salesforce edition you have.

USER PERMISSIONS

To find permissions and settings in a profile:

- [View Setup and Configuration](#)

Item	Search for	Example
Tabs	Tab or parent object name	Type <code>rep</code> , then select <code>Reports</code> .
App and system permissions	Permission name	Type <code>api</code> , then select <code>API Enabled</code> .
All other categories	Category name	To find Apex class access settings, type <code>apex</code> , then select <code>Apex Class Access</code> . To find custom permissions, type <code>cust</code> , then select <code>Custom Permissions</code> . And so on.

If no results appear in a search:

- Check if the permission, object, tab, or setting you're searching for is available in the current organization.
- Verify that the item you're searching for is available for the user license that's associated with the current profile. For example, a profile with the High Volume Customer Portal license doesn't include the "Modify All Data" permission.
- Ensure that your search term contains at least three consecutive characters that match the name of the item you want to find.
- Make sure that you spelled the search term correctly.

SEE ALSO:

[Enable the Enhanced Profile User Interface](#)

Permission Sets

A permission set is a collection of settings and permissions that give users access to various tools and functions. Permission sets extend users' functional access without changing their profiles and are the recommended way to manage your users' permissions.

Watch how you can grant users permissions using permission sets.

 [Watch a video](#)

Users can have only one profile but, depending on the Salesforce edition, they can have multiple permission sets. You can assign permission sets to various types of users, regardless of their profiles.

Create permission sets to grant access for a specific job or task, regardless of the primary job function or title of the users they're assigned to. For example, let's say you have several users who must delete and transfer leads. You can create a permission set based on the tasks that these users must perform and include the permission set within permission set groups based on the users' job functions.

If a permission isn't enabled in a profile but is enabled in a permission set, users with that profile and permission set have the permission. For example, if Manage Password Policies isn't enabled in a user's profile but is enabled in one of their permission sets, they can manage password policies.

A permission set's overview page provides an entry point for all of the permissions in a permission set. To open a permission set overview page, from Setup, enter `Permission Sets` in the Quick Find box, then select **Permission Sets** and select the permission set you want to view.

[Guidelines for Creating Permission Sets and Permission Set Groups](#)

Review these recommendations on setting up your permission sets and permission set groups.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

[Create Permission Sets](#)

Create permission sets that contain the permissions necessary for your users to complete a specific job or task.

[Configure Permissions and Access in Permission Sets](#)

Configure object, field, and user permissions as well as other access and feature settings in permission sets.

[Manage Permission Set Assignments](#)

You can assign permission sets to a single user from the user detail page or assign multiple users to a permission set from any permission set page.

[Types of Permission Sets](#)

Salesforce offers several types of permission sets to help your users achieve their business goals.

[Permission Set Considerations](#)

Be aware of these considerations and special behaviors for permission sets.

[Standard Permission Sets](#)

A standard permission set consists of a group of common permissions for a particular feature associated with a permission set license. Using a standard permission set saves you time and facilitates administration because you don't need to create the custom permission set.

[Integration Permission Sets](#)

Integration permission sets define the scope of data access by Salesforce integration-related features and services.

[Session-Based Permission Sets](#)

A session-based permission set applies to a specific user session to grant someone functional access to permissions.

[View Permissions Enabled in a Permission Set \(Beta\)](#)

To help you manage your permission sets, you can see all object, user, and field permissions that are enabled for a permission set in its summary page.

[See the Count of Permission Set Groups a Permission Set Is Added To](#)

See how many permission set groups a specific permission set is included in. This count can help you to estimate the potential impact on your users before making a change to a permission set.

[Work with Permission Set Lists](#)

Create list views to help view and manage your permission sets. You can also edit permissions in multiple permission sets at the same time using list views.

[Search Permission Sets](#)

To quickly navigate to other pages in a permission set, you can enter search terms in any permission set detail page.

[Report on Custom Permission Set and Permission Set Group Assignments](#)

To help you manage users, report on your users' assigned custom permission set and permission set groups. Create a custom report type before building reports on custom permission set or permission set group assignments.

Guidelines for Creating Permission Sets and Permission Set Groups

Review these recommendations on setting up your permission sets and permission set groups.

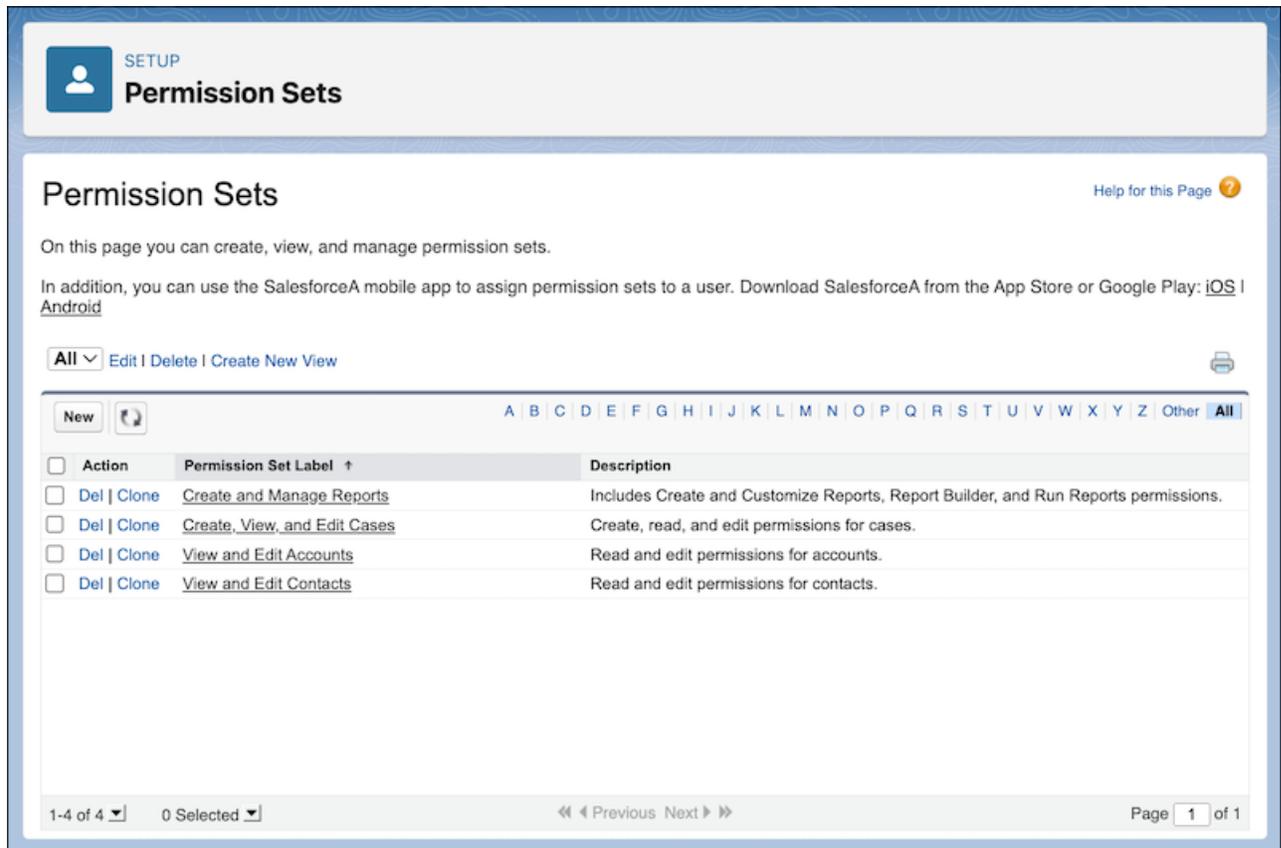
- When possible, assign users the Minimum Access - Salesforce profile, and then use permission sets and permission set groups to grant users only the permissions that they require. Apply permission sets to users based on the tasks that they do rather than their job title. Because you can reuse smaller permission set building blocks, you can avoid creating dozens or even hundreds of profiles for each user and job function.
 - Create permission sets that include all permissions necessary for a job or task. Then bundle these permission sets into permission set groups that correspond to your user personas. If different personas perform some of the same tasks, you can reuse those permission sets in different permission set groups. If a user has more than one persona, you can assign them multiple permission set groups.
 - To remove permissions from a permission set group without affecting the included permission sets, create a muting permission set. You don't need to create nearly identical permission sets with only those few permissions removed.
 - Use a naming structure that clearly identifies the contents of each permission set.
 - Configure these permissions and features in permission sets.
 - Apex classes
 - Connected app access
 - Custom permissions
 - Field permissions
 - Object permissions
 - User permissions (app permissions and system permissions)
 - Tab settings
 - Visualforce pages
 - Configure these features in profiles.
 - Default apps and record types
 - IP ranges
 - Login hours
 - Page layout assignment
 - To set field-level security on permission sets instead of profiles, enable **Field-Level Security for Permission Sets During Field Creation**.
 - To set assignments to end on a specific date, enable **Permission Set & Permission Set Group Assignments with Expiration Dates**. For short-term tasks or projects with a fixed end date, you can limit user permissions to match and save time cleaning up your users' access after the work ends.
-  **Example:** You're setting up access for your IT Help Desk team. This team views and edits accounts and contacts and creates, views, and edits cases. The team also creates and manages reports. Assign all members on this team the Minimum Access - Salesforce profile. To configure the permissions required to complete these tasks, create these permission sets.
- View and Edit Accounts, which includes read and edit permissions for accounts. You also set the account field permissions so that the team can view and edit the fields required for their work.
 - View and Edit Contacts, which includes read and edit permissions for contacts. You also set the contact field permissions so that the team can view and edit the fields required for their work.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

- Create, View, and Edit Cases, which includes create, read, and edit permissions for cases. You also set the case field permissions so that the team can view and edit the fields required for their work.
- Create and Manage Reports, which includes the Create and Customize Reports, Report Builder, and Run Reports permissions.



SETUP
Permission Sets

Permission Sets [Help for this Page](#)

On this page you can create, view, and manage permission sets.

In addition, you can use the SalesforceA mobile app to assign permission sets to a user. Download SalesforceA from the App Store or Google Play: [iOS](#) | [Android](#)

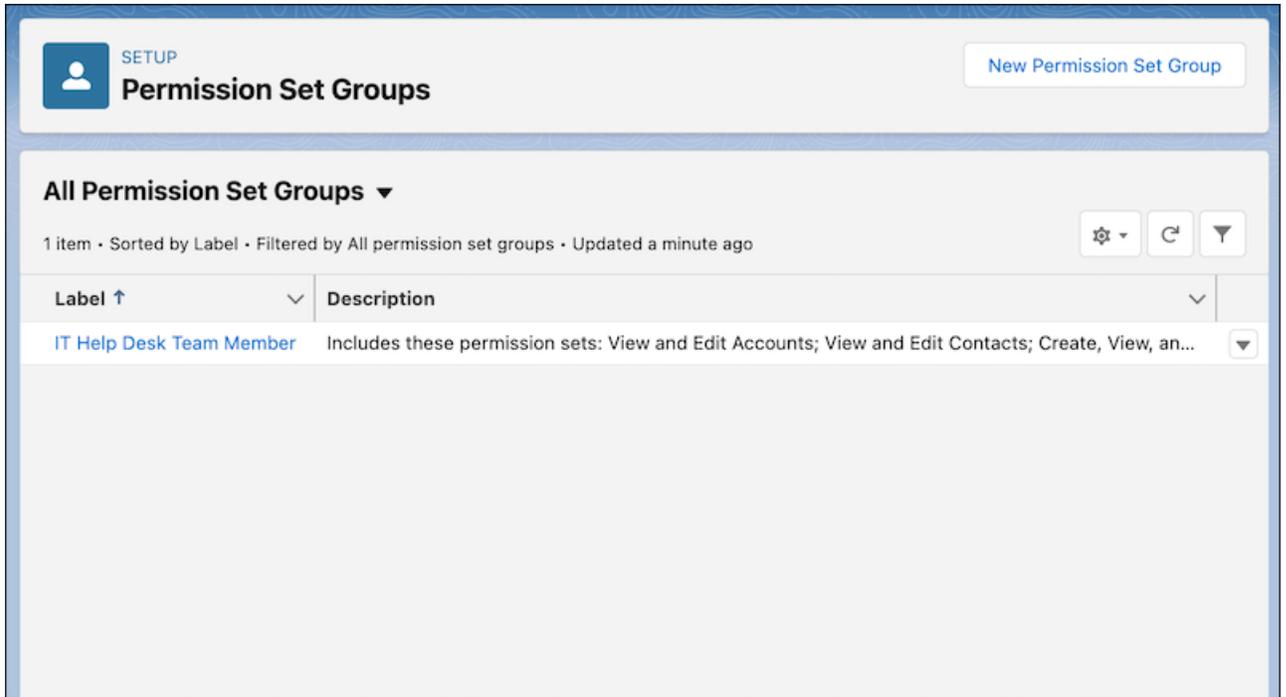
All | Edit | Delete | Create New View

New  [A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#) [Other](#) **All**

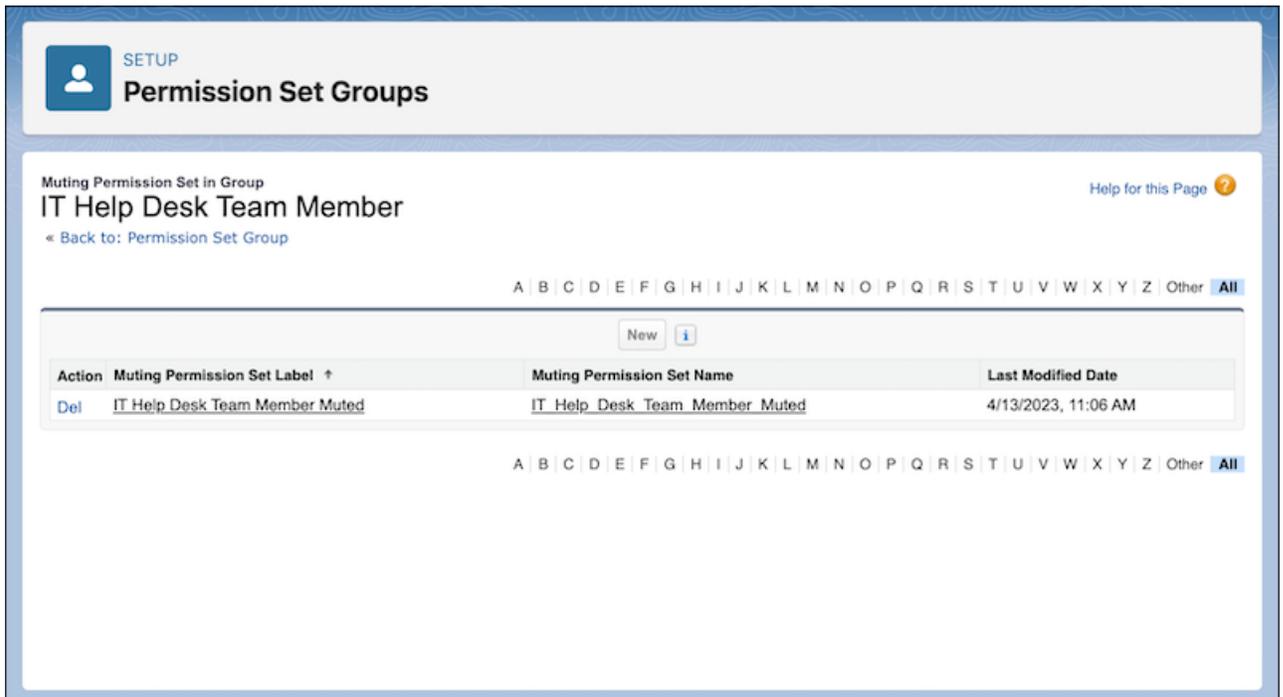
<input type="checkbox"/>	Action	Permission Set Label ↑	Description
<input type="checkbox"/>	Del Clone	Create and Manage Reports	Includes Create and Customize Reports, Report Builder, and Run Reports permissions.
<input type="checkbox"/>	Del Clone	Create, View, and Edit Cases	Create, read, and edit permissions for cases.
<input type="checkbox"/>	Del Clone	View and Edit Accounts	Read and edit permissions for accounts.
<input type="checkbox"/>	Del Clone	View and Edit Contacts	Read and edit permissions for contacts.

1-4 of 4 | 0 Selected | << Previous Next >> | Page 1 of 1

Then you add all four permission sets to a new permission set group named IT Help Desk Team Member. If other personas on other teams perform the same tasks, you can reuse these permission sets in different permission set groups designated for these users.



Before you assign users to the permission set group, you review the fields visible via the included permission set. You realize that you don't want this team to see the Account Revenue field on account records. But you don't want to remove the read access for this field from the View and Edit Accounts permission set because other personas who are assigned this permission set through other permission set groups still need this field. You create a muting permission set in the IT Help Desk Team Member permission set group.



Then remove read access for the Account Revenue field.

SETUP
Permission Set Groups

Muting Permission Set in Groups
IT Help Desk Team Member
[← Back to: Permission Set Group](#)

Find Settings... | Edit Properties

Muting Permission Set Overview > Object Settings ▾ **Accounts** ▾

Accounts Save Cancel

Tab Settings

Available	Visible	Muted
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Object Permissions

Permission Name	Enabled	Muted
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Create	<input type="checkbox"/>	<input type="checkbox"/>
Edit	<input type="checkbox"/>	<input type="checkbox"/>
Delete	<input type="checkbox"/>	<input type="checkbox"/>
View All	<input type="checkbox"/>	<input type="checkbox"/>
Modify All	<input type="checkbox"/>	<input type="checkbox"/>

Field Permissions

Field Name	Read Access	Edit Access	Read Access Muted	Edit Access Muted
Account Name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Account Number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Account Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Account Site	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Account Source	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Active	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Annual Revenue	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Your company is making some changes, so you expect higher than usual cases for a few weeks and want more users to assist the IT Help Desk team during this time. You assign these users the IT Help Desk Team Member permission set group as well, but you set an expiration date for the assignment. After the expiration date, these users are automatically unassigned from the permission set group and no longer have the included permissions.

... > PERMISSION SET GROUP 'IT HELP DESK TEAM MEMBER' > MANAGE ASSIGNMENT EXPIRATION

IT Help Desk Team Member

Select an Expiration Option For Assigned Users

No expiration date ⓘ

 Specify the expiration date

ⓘ

ⓘ

Selected Users

Full Name	Role	Profile	Active	User License	Expires On	Time Zone
Andrea Kim	Customer Support, North America	Minimum Access - Salesforce	✓	Salesforce	May 30, 2023	America/Los_Ar
Steven Smith	Customer Support, North America	Minimum Access - Salesforce	✓	Salesforce	May 30, 2023	America/Los_Ar

Create Permission Sets

Create permission sets that contain the permissions necessary for your users to complete a specific job or task.

You can clone a permission set or create one. A cloned permission set starts with the same licenses and enabled permissions as the original one. A new permission set starts with no licenses selected and no permissions enabled.

Tip: If your org has many permission sets, using permission set groups can help improve performance.

1. From Setup, in the Quick Find box, enter *Permission Sets*, and then select **Permission Sets**.
2. Click **New**.
3. Enter your permission set information.
4. Select the types of users for the permission set. Select a specific user or permission set license. Or, if users with different licenses are assigned the permission set, select **None**. If the permission set is associated with a specific license, it can only include the permission and settings entitled by that license.

When creating a permission set for a specific permission set license, refer to that feature's documentation. For example, to create a permission set for the Identity Connect permission set license, use these steps along with the Identity Connect documentation.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To create permission sets:

- Manage Profiles and Permission Sets

To assign permission sets:

- Assign Permission Sets

5. Add the required permissions and settings to the permission set. For more information, see [Configure Permissions and Access in Permission Sets](#) in Salesforce Help.

 **Example:** You have several Sales Users who are currently allowed to read, create, and edit leads. But you need some users to also delete and transfer leads. You create a permission set for this specific task. Under Object Settings, select Leads and enable delete. Under App Permissions, find and enable the Transfer Leads permission. Assign the permission set to users who need these permissions.

SEE ALSO:

[Guidelines for Creating Permission Sets and Permission Set Groups](#)

[Permission Sets](#)

[Create a Permission Set Associated with a Permission Set License](#)

[Permission Set Licenses](#)

[Permission Set Groups](#)

Configure Permissions and Access in Permission Sets

Configure object, field, and user permissions as well as other access and feature settings in permission sets.

Create permission sets that contain all the permission and settings for a specific job or task. In permission sets, you can configure the following:

- [Object permissions](#)
- [User permissions](#) (app permissions and system permissions)
- [Field permissions](#)
- [Custom permissions](#)
- [Tab settings](#)
- [Record types](#) (not defaults)
- [Visualforce page access](#)
- [Apex class access](#)
- [Connected app access](#)
- [Assigned apps](#)

Depending on your Salesforce org, settings for other features and apps are available to configure in permission sets.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

Enable Object Permissions in Permission Sets

Object permissions determine the base-level access users have to create, read, edit, and delete records for each object. Permission sets are the recommended feature for managing object permissions.

1. From Setup, in the Quick Find box, enter *Permission Sets*, and then select **Permission Sets**.
2. Select a permission set.
3. In the Find Settings... box, enter the name of the object and select it from the list. Click **Edit**.
4. In the Object Permissions section, enable the desired permissions.
5. Click **Save**.

On the object's page, you can also edit tab settings, record type settings, and field permissions.

SEE ALSO:

- [Object Permissions](#)
- [Configure Permissions and Access in Permission Sets](#)
- [Permission Sets](#)
- [Enable User Permissions in Permission Sets](#)

Enable User Permissions in Permission Sets

User permissions specify what tasks users can perform and what features users can access. In permission sets, you enable user permissions in the App Permissions and System Permissions sections.

1. From Setup, in the Quick Find box, enter *Permission Sets*, and then select **Permission Sets**.
2. Select a permission set.
3. On the permission set overview page, search for the user permission that you want to enable in the Find Settings... box, and then select it.
4. On the App Permissions or System Permissions page, click **Edit**.
5. Scroll down to the user permission and select its checkbox.
6. Click **Save**.

SEE ALSO:

- [Configure Permissions and Access in Permission Sets](#)
- [Permission Sets](#)
- [User Permissions](#)
- [Enable Object Permissions in Permission Sets](#)

EDITIONS

Available in: Salesforce Classic (**not available in all orgs**) and Lightning Experience

The available object settings vary according to which Salesforce edition you have.

Permission sets available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

USER PERMISSIONS

To view object settings:

- View Setup and Configuration

EDITIONS

Available in: both Salesforce Classic (**not available in all orgs**) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

USER PERMISSIONS

To edit user permissions:

- Manage Profiles and Permission Sets

Enable Custom Permissions in Permission Sets

Custom permissions give you a way to provide access to custom processes or apps. After you've created a custom permission and associated it with a process or app, you can enable the permission in permission sets.

1. From Setup, enter *Permission Sets* in the Quick Find box, then select **Permission Sets**.
2. Select a permission set, or create one.
3. On the permission set overview page, click **Custom Permissions**.
4. Click **Edit**.
5. To enable custom permissions, select them from the Available Custom Permissions list and then click **Add**. To remove custom permissions from the permission set, select them from the Enabled Custom Permissions list and then click **Remove**.
6. Click **Save**.

SEE ALSO:

[Configure Permissions and Access in Permission Sets Custom Permissions](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

In Group and Professional Edition organizations, you can't create or edit custom permissions, but you can install them as part of a managed package.

USER PERMISSIONS

To enable custom permissions in permission sets:

- [Manage Profiles and Permission Sets](#)

View and Edit Tab Settings in Permission Sets

Tab settings specify whether a tab appears in the All Tabs page or is visible in a tab set.

1. From Setup, in the Quick Find box, enter *Permission Sets*, and then select **Permission Sets**.
2. Select a permission set.
3. In the Find Settings... box, enter the name of the object you want and select it from the list, then click **Edit**.
4. [Specify the tab settings](#).
5. Click **Save**.

 **Note:** If Salesforce CRM Content is enabled for your organization but the **Salesforce CRM Content User** checkbox isn't enabled on the user detail page, the Salesforce CRM Content app has no tabs.

Tab Settings

Tab settings specify whether a tab is visible in its associated app. They also determine whether a tab appears in the All Tabs page in Salesforce Classic and whether objects appear in the Lightning Experience App Launcher and navigation menus. Tab settings labels in permission sets differ from the labels in profiles.

SEE ALSO:

[Configure Permissions and Access in Permission Sets](#)
[Permission Sets](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Tab settings available in: **All Editions** except **Database.com**

Permission sets available in: **Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

Profiles available in: **Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To view tab settings:

- View Setup and Configuration

To edit tab settings:

- Manage Profiles and Permission Sets

Tab Settings

Tab settings specify whether a tab is visible in its associated app. They also determine whether a tab appears in the All Tabs page in Salesforce Classic and whether objects appear in the Lightning Experience App Launcher and navigation menus. Tab settings labels in permission sets differ from the labels in profiles.

Enabled Settings in Permission Sets	Enabled Setting in Profiles	Description
Available	Default Off	<p>The tab doesn't appear in an app's navigation bar, but it's available in the App Launcher in Lightning Experience and on the All Tabs page in Salesforce Classic.</p> <p>Individual users can customize their display to make the tab visible in any app.</p>
Available and Visible	Default On	<p>The tab appears in an app's navigation bar. The tab is also available in the App Launcher in Lightning Experience and on the All Tabs page in Salesforce Classic.</p> <p>Individual users can customize their display to hide the tab or make it visible in other apps.</p>
None	Tab Hidden	<p>The tab isn't available in the App Launcher or the All Tabs page, isn't visible in any app navigation, and is excluded from API responses.</p>

If a user has another permission set or profile with enabled settings for the same tab, the most permissive setting applies. For example, let's say permission set A has no settings enabled for the Accounts tab and permission set B enables the `Available` setting for the Accounts tab. If permission sets A and B are assigned to a user, the user sees the Accounts tab on the All Tabs page.

SEE ALSO:

[View and Edit Tab Settings in Permission Sets](#)

EDITIONS

Available in: Salesforce Classic and Lightning Experience ([not available in all orgs](#))

Tab settings available in: **All Editions** except **Database.com**

Permission sets available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com Editions**

Profiles available in: **Professional, Enterprise, Performance, Unlimited, Developer, and Database.com Editions**

Set Visualforce Page Access in Permission Sets

You can specify access to Visualforce pages in permission sets.

1. From Setup, in the Quick Find box, enter *Permission Sets*, and then select **Permission Sets**.
2. Select a permission set.
3. Click **Visualforce Page Access**.
4. Click **Edit**.
5. Select the Visualforce pages that you want to enable from the Available Visualforce Pages list and click **Add**, or select the Visualforce pages that you want to disable from the Enabled Visualforce Pages list and click **Remove**.
6. Click **Save**.

SEE ALSO:

[Configure Permissions and Access in Permission Sets](#)
[Permission Sets](#)

App and System Settings in Permission Sets

In permission sets, permissions and settings are organized into app and system categories. These categories reflect the rights users need to administer and use system and app resources.

App Settings

Apps are sets of tabs that users can change by selecting the drop-down menu in the header. All underlying objects, components, data, and configurations remain the same, regardless of the selected app. In selecting an app, users navigate in a set of tabs that allows them to efficiently use the underlying functionality for app-specific tasks. For example, let's say you do most of your work in the sales app, which includes tabs like Accounts and Opportunities. To track a new marketing campaign, rather than adding the Campaigns tab to the sales app, you select Marketing from the app drop-down to view your campaigns and campaign members.

The Apps section of the permission sets overview page contains settings that are directly associated with the business processes the apps enable. For example, customer service agents might need to manage cases, so the "Manage Cases" permission is in the Call Center section of the App Permissions page. Some app settings aren't related to app permissions. For example, to enable the Time-Off Manager app from the AppExchange, users need access to the appropriate Apex classes and Visualforce pages, as well as the object and field permissions that allow them to create new time-off requests.

System Settings

Some system functions apply to an organization and not to any single app. For example, "View Setup and Configuration" allows users to view setup and administrative settings pages. Other system functions apply to all apps. For example, the "Run Reports" and "Manage

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To view Visualforce page access settings:

- View Setup and Configuration

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

Dashboards" permissions allow managers to create and manage reports in all apps. In some cases, such as with "Modify All Data," a permission applies to all apps, but also includes non-app functions, like the ability to download the Data Loader.

SEE ALSO:

[Configure Permissions and Access in Permission Sets](#)
[Permission Sets](#)

Assign Custom Record Types in Permission Sets

You can assign record types to users in permission sets.

1. From Setup, in the Quick Find box, enter *Permission Sets*, and then select **Permission Sets**.
2. Select a permission set, or create one.
3. On the permission set overview page, click **Object Settings**, then click the object you want.
4. Click **Edit**.
5. Select the record types you want to assign to this permission set.
6. Click **Save**.

How Is Record Type Access Specified?

Assign record types to users in their profiles or permission sets (or permission set groups), or a combination of these. Record type assignment behaves differently in profiles and permission sets.

SEE ALSO:

[Assign Record Types and Page Layouts in Profiles](#)

How Is Record Type Access Specified?

Assign record types to users in their profiles or permission sets (or permission set groups), or a combination of these. Record type assignment behaves differently in profiles and permission sets.

Before assigning a record type, understand the different types available in your Salesforce org. The behavior for record creation depends on which record types are assigned and if you assign them via profiles or permission sets (or permission set groups).

- **Default Record Types:** A user's default record type is specified in the user's profile. Users can view their default record type and edit record type selection in personal settings. You can't specify a default record type in permission sets.
- **Master Record Types:**
 - In Profiles: You can assign the master record type in profiles, but you can't include custom record types in the profile.
 - In Permission Sets: You can assign only custom record types in permission sets, not master record types.

This chart includes examples of what happens when users create records with different combinations of record type assignments.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Record types available in: **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To assign record types in permission sets:

- Manage Profiles and Permission Sets

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited,** and **Developer** editions

Record Type Assigned on Profile	Custom Record Types in Permission Set (or Permission Set Group) Assigned	What Happens When a User Creates a Record
--Master--	None	The new record is associated with the Master record type.
--Master--	One	The new record is associated with the custom record type. Users can't select the Master record type.
--Master--	Multiple	Users are prompted to select a record type.
Custom	One or more	Users are prompted to select a record type. In their personal settings, users can set an option to use their default record type and not be prompted to choose a record type.

When working with record type assignments, keep the following considerations in mind:

- Page layout assignments are specified in profiles only, not in permission sets. When a permission set specifies a custom record type, users with that permission set get the page layout assignment that's specified for that record type in their profile. In profiles, page layout assignments are specified for every record type, even when record types aren't assigned.
- Lead conversion default record types are specified in a user's profile for the converted records. During lead conversion, the display of the user's available record types is unsorted.
- Record type assignment on a user's profile or permission set (or permission set group) doesn't determine whether a user can view a record with that record type. The record type assignment simply specifies that the user can use that record type when creating or editing a record.

SEE ALSO:

[Assign Record Types and Page Layouts in Profiles](#)

[Assign Custom Record Types in Permission Sets](#)

View and Edit Assigned Apps in Permission Sets

Assigned app settings specify the apps that users can select in the Lightning Platform app menu.

Unlike profiles, you can't assign a default app in permission sets. You can only specify whether apps are visible.

To assign apps:

1. From Setup, in the Quick Find box, enter *Permission Sets*, and then select **Permission Sets**.
2. Select a permission set, or create one.
3. On the permission set overview page, click **Assigned Apps**.
4. Click **Edit**.
5. To assign apps, select them from the Available Apps list and click **Add**. To remove apps from the permission set, select them from the Enabled Apps list and click **Remove**.
6. Click **Save**.

SEE ALSO:

- [View and Edit Assigned Apps in Profiles](#)
- [Configure Permissions and Access in Permission Sets](#)
- [Permission Sets](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To edit assigned app settings:

- [Manage Profiles and Permission Sets](#)

Manage Permission Set Assignments

You can assign permission sets to a single user from the user detail page or assign multiple users to a permission set from any permission set page.

 **Note:** Some permissions require users to have a specific user license or permission set license before you can grant them in permission sets. For example, if you add the Use Identity Connect user permission to the Identity permission set, you can assign only users with the Identity Connect permission set license to the permission set. Or, if you create a permission set without specifying a license and include the Author Apex permission, you can't assign the permission set to Salesforce Platform users, because their user license doesn't allow Apex authoring.

[Assign Permission Sets to a Single User](#)

Assign permission sets or remove permission set assignments for a single user from the user detail page.

[Assign a Permission Set to Multiple Users](#)

Assign a permission set to one or more users from any permission set page.

[Remove User Assignments from a Permission Set](#)

From any permission set page, you can remove the permission set assignment from one or more users.

Assign Permission Sets to a Single User

Assign permission sets or remove permission set assignments for a single user from the user detail page.

1. From Setup, in the Quick Find box, enter *Users*, and then select **Users**.
2. Select a user.
3. In the Permission Set Assignments related list, click **Edit Assignments**.
4. To assign a permission set, select it under Available Permission Sets and click **Add**. To remove a permission set assignment, select it under Enabled Permission Sets and click **Remove**.
5. Click **Save**.

Assign a Permission Set to Multiple Users

Assign a permission set to one or more users from any permission set page.

1. From Setup, in the Quick Find box, enter *Permission Sets*, and then click **Permission Sets**.
2. Select the permission set that you want to assign to users.
3. Click **Manage Assignments** and then **Add Assignments**.
4. Select the checkboxes next to the names of the users you want assigned to the permission set, and click **Next**.
5. Optionally, select an expiration date for the user assignment to expire. For more information, see [Permission Set and Permission Set Group Assignment Expiration](#) in Salesforce Help.
6. Click **Assign**.

Messages confirm success or indicate if a user doesn't have the appropriate licenses for assignment.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To assign permission sets:

- Assign Permission Sets
- AND
- View Setup and Configuration

To remove permission set assignments:

- Assign Permission Sets

Remove User Assignments from a Permission Set

From any permission set page, you can remove the permission set assignment from one or more users.

1. From Setup, in the Quick Find box, enter *Permission Sets*, and then select **Permission Sets**.
2. Select a permission set.
3. In the permission set toolbar, click **Manage Assignments**.
4. Select the users to remove from this permission set. You can remove up to 1,000 users at a time.
5. Click **Remove Assignments**.
6. To return to a list of all users assigned to the permission set, click **Done**.

Types of Permission Sets

Salesforce offers several types of permission sets to help your users achieve their business goals.

Depending on what you and your users want to do, you can employ a combination of permission set types when administering your Salesforce org. Salesforce offers the following permission set options.

Permission Set Type	Description	Typical Use Case
Custom Permission Set	Created by administrators based on tasks that users perform.	Users who perform the same tasks but have different personas or roles. For example, sometimes users who create and edit contracts are in separate departments. Create a permission set for the tasks, and then include the permission set in appropriate permission set groups based on their personas.
Integration Permission Set	Offered by Salesforce for specific integrations. Only certain permission types can be modified by your org. The editability is based on the specific integration's use case.	You connect to the cloud to exchange data with integration partners. Integration permission sets define the scope of data access by Salesforce integration-related features and services. Depending on the integration features, integration permission sets can: <ul style="list-style-type: none"> • be predefined by Salesforce but aren't editable by your org. • have no initial permissions and be fully controlled by your org.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

Permission Set Type	Description	Typical Use Case
		<ul style="list-style-type: none"> come with on-premises permissions but can be modified by you.
Managed Permission Set	Installed from a managed package and has the package namespace.	Package developers include entitlements to access features in a managed package. Permissions in these permission sets aren't editable by subscriber orgs.
Session-Based Permission Set	Allows functional access only during a predefined session type.	You limit access to functionality for more security. Or, you sometimes limit access to equipment to users in certain roles. For example, let's say your org has a custom object called Conference Room. A mobile app called Conference Room Sync has read and update access to the object. You can create a permission set to allow updates to the object only when the Conference Room Sync connected mobile app generates the user's session.
Standard Permission Set	Includes common permissions for a feature associated with a permission set license. Using standard instead of custom permission sets saves time and facilitates administration. For more information, see Standard Permission Sets in Salesforce Help.	Users who require permissions for a permission set license.

SEE ALSO:

[Permission Sets](#)

Permission Set Considerations

Be aware of these considerations and special behaviors for permission sets.

Apex Class Access

- You can specify which methods in a top-level Apex class are executable for a permission set. Apex class access settings apply only to:
 - Apex class methods, such as Web service methods
 - Any method used in a custom Visualforce controller or controller extension applied to a Visualforce page
- Triggers always fire on trigger events (such as `insert` or `update`), regardless of permission settings.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

Assigned Apps

Assigned app settings specify the apps that users can select in the Lightning Platform app menu. Unlike profiles, you can't assign a default app in permission sets. You can only specify whether apps are visible.

Experience Cloud Sites

Permission sets can be assigned to a site's membership, granting users who are assigned to the permission set access to the site. If you add a permission to a permission set that is being used to grant membership to a site, the site members also get access to the permissions unrelated to the site membership. Salesforce recommends checking if a permission set is used in any site's membership list before adding new permissions to it.

You can't use permission set groups to add membership to a site, only permission sets.

Limits

Make sure to refer to the Salesforce Features and Editions Limits for your specific edition.

New and Cloned Permission Sets

A new permission set starts with no user license selected and no permissions enabled. A cloned permission set has the same user license and enabled permissions as the permission set that it's cloned from. You can't change the user license in a cloned permission set. Clone a permission set only if the new one requires the same user license as the original.

Object Permissions

A profile or a permission set can have an entity, such as Account, with a master-detail relationship. A broken permission dependency exists if the child entity has permissions that the parent should have. Salesforce updates the parent entity for a broken permission dependency on the first save action for the profile or permission set.

If the child entity has these permissions	These permissions are enabled on the parent entity
Modify All OR View All	View All
View All OR Read	Read

Permission Set Groups

If your org has many permission sets, using permission set groups can help improve performance.

Permission Set Licenses

In API version 38.0 and later, you can create a permission set and associate it with a permission set license. When you create a permission set using a specific permission set license, users assigned to the permission set receive all functionality associated with the permission set license.

Profiles

In API version 25.0 and later, every profile is automatically associated with a permission set, whether you explicitly assign it to one or not. This permission set stores the profile's user, object, and field permissions, plus setup entity access settings. You can query on these profile-owned permission sets but not modify them. They're not visible in the user interface.

User License Restrictions

Some user licenses restrict the number of custom apps or tabs that a user can access. In this case, you can assign only the allotted number through the user's assigned profile and permission sets. For example, a user with the App Subscription user license with access to one Light App can access only that app's custom tabs.

SEE ALSO:

[Permission Set Groups](#)

[How Is Record Type Access Specified?](#)

[Object Permissions](#)

[Salesforce Features and Edition Allocations](#)

Standard Permission Sets

A standard permission set consists of a group of common permissions for a particular feature associated with a permission set license. Using a standard permission set saves you time and facilitates administration because you don't need to create the custom permission set.

To see which permission sets are standard, add **Is Custom** to your list view. The **Is Custom** box isn't checked for standard permission set. Permission sets you created or cloned are indicated with a checkmark.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

The screenshot shows the 'Permission Sets' page in Salesforce. The view is 'Standard Perm Sets (IsCustor)'. The table below shows the following data:

Action	Permission Set Label	Is Custom
Del Clone	Finance Users	✓
Del Clone	IdentityConnect	✓
Del Clone	Salesforce Console Sales Reps	✓
Clone	Salesforce Console User	<input type="checkbox"/>

Standard permission sets don't count against your org's permission set limits. You can clone a standard permission set as many times as you want, but you can't edit it. Clones do count against your org's permission set limits.

Example: Let's say you purchased 10 Sales Console User permission set licenses. You can do any of the following.

- Assign all 10 users to the Salesforce Console User permission set.

- Assign some of the users to the Salesforce Console User permission set, and assign the remainder to a clone of Salesforce Console User.
- Clone the Salesforce Console User permission set and assign different users to each clone, based on your org's structure.

Integration Permission Sets

Integration permission sets define the scope of data access by Salesforce integration-related features and services.

Use integration permission sets if you connect to the cloud to exchange data with integration partners. Depending on the integration features, integration permission sets can:

- be predefined by Salesforce but aren't editable by your org.
- have no initial permissions and be fully controlled by your org.
- come with on-premises permissions but can be modified by you.
- be partially editable.

Session-Based Permission Sets

A session-based permission set applies to a specific user session to grant someone functional access to permissions.

Let's say your org has a custom object named Conference Room. A mobile app called Conference Room Sync has read and update access to the object. You can create a permission set to allow updates to the object only when the Conference Room Sync connected mobile app generates the user's session.

Or perhaps you have a web application that accesses confidential information. For security reasons, you want to limit user access to a predetermined length of time. You can create a session-based permission set that activates only when users authenticate into your environment using a token. When the token expires, the user must reauthenticate to access the application again.

You can also use session-based permission sets in Flow Builder. For example, you have a junior buyer in your org who occasionally requires access to your Contracts object. Create a session-based permission set with access to the object, and then create a flow that uses the Activate Session-Based Permission Set action available in Flow Builder. In the flow, pass the permission name to the action. During runtime, the action checks who's running the flow. When the flow runs, the activation process fires. After the flow completes, the buyer has access to the Contracts object for the current session.

To activate session-based permission sets via REST API or SOAP API, see the [SessionPermSetActivation](#) object in the *Object Reference*. You need the Manage Session Permission Set Activation permission.

Before assigning session-based permission sets to users, ensure that they can meet the conditions of the permission set. For example, grant user access to appropriate tools, such as authenticators. As a best practice, inform users of the conditions in which they can access certain applications and tools. User assignment information appears on the user detail page in a related list called Permission Set Assignments: Activation Required.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

Action	Permission Set Label	Date Assigned
Del	IdentityConnectPSL	4/1/2016

Action	Permission Set Label	Date Assigned
Del	Exec_Conference_Rm_Permission	4/1/2016

Tip: When you create your permission set list view, select columns to include **Session Activation Required** to view which permission sets are session-based.

Create a Flow That Can Activate or Deactivate a Session-Based Permission Set

You can create a session-based permission set and then create a flow that users can run to activate or deactivate the permission set themselves.

Create a Flow That Can Activate or Deactivate a Session-Based Permission Set

You can create a session-based permission set and then create a flow that users can run to activate or deactivate the permission set themselves.

Before beginning, check out [Session-Based Permission Sets](#) to learn when to use them.

Important: You can run queries, however, don't make data or object updates in flows that also activate session-based permission sets.

You can't both activate and deactivate a session-based permission set in the same flow. You must create separate flows for these actions.

1. [Create a permission set](#) and make sure to select **Session Activation Required**.
2. [Assign the permission set to users](#).
3. [Create a flow](#) in Flow Builder.
 - a. Use a Get Records element to look up the permission set.
 - b. In the Get Records element, store the permission set's name in a variable, so that you can use the name in the action.
 - c. Drag a Core Action element onto the canvas, and choose either **Activate Session-Based Permission Set** or **Deactivate Session-Based Permission Set**.
4. Activate your flow.
5. [Distribute your flow](#) to users who must run it.

Example: Create a flow to pass a permission name to the Activate Session-Based Permission Set core action. First, add a Get Records element to your flow to look up the PermissionSet object. Set the Name field to the name of your session-based permission set. Then add the Activate Session-Based Permission Set core action, and set the input to your permission set name.

Tip: Make sure that users who run your flow have the Run Flows permission.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To create permission sets:

- Manage Profiles and Permission Sets

To assign permission sets:

- Assign Permission Sets

To open, edit, or create a flow in Flow Builder:

- Manage Flow

When the flow activates the session-based permission set, the running user obtains access to the permissions specified in your permission set during the current user session. If the flow deactivates the session-based permission set, the permissions are no longer available to the user.

SEE ALSO:

[Permission Sets](#)

[Session-Based Permission Sets](#)

[Flow Core Action: Activate Session-Based Permission Set](#)

[Flow Core Action: Deactivate Session-Based Permission Set](#)

View Permissions Enabled in a Permission Set (Beta)

To help you manage your permission sets, you can see all object, user, and field permissions that are enabled for a permission set in its summary page.

 **Note:** This feature is a Beta Service. Customer may opt to try such Beta Service in its sole discretion. Any use of the Beta Service is subject to the applicable Beta Services Terms provided at Agreements and Terms.

1. From Setup, in the Quick Find box, enter *Permission Sets*, and then select **Permission Sets**.
2. Select a permission set.
3. Click **View Summary (Beta)**. On this page, you can see details about the permission set, its related permission set groups, and its included object, user, and field permissions.

 **Note:** For standard permission sets, the Created Date is the Salesforce org's creation date.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To view and manage permission sets:

- View Setup and Configuration

See the Count of Permission Set Groups a Permission Set Is Added To

See how many permission set groups a specific permission set is included in. This count can help you to estimate the potential impact on your users before making a change to a permission set.

1. From Setup, in the Quick Find box, enter *Permission Sets*, and then select **Permission Sets**.
2. Select a permission set.
3. View the count in the Permission Set Groups Added To field.

SEE ALSO:

[Add Permission Sets to a Permission Set Group](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To create permission sets:

- Manage Profiles and Permission Sets

To assign permission sets:

- Assign Permission Sets

To create a permission set group:

- Manage Profiles and Permission Sets

Work with Permission Set Lists

Create list views to help view and manage your permission sets. You can also edit permissions in multiple permission sets at the same time using list views.

Create and Edit Permission Set List Views

You can create permission set list views to view a set of permission sets with the fields that you choose.

1. From Setup, in the Quick Find box, enter *Permission Sets*, and then select **Permission Sets**.
2. In the Permission Sets detail page, click **Create New View**, or select a view and click **Edit**.
3. Enter the view name.
4. Under Specify Filter Criteria, specify the conditions that the list items must match, such as *Modify All Data equals True*.
 - a. To search for and select the setting you want, type a setting name, or click the lookup icon.
 - b. Choose a filter operator.
 - c. Enter the value that you want to match.
 - d. To specify another filter condition, click **Add New**. You can specify up to 25 filter condition rows.
5. Under Select Columns to Display, specify the permission set settings that you want to appear as columns in the list view. You can add up to 15 columns in a single list view.
 - a. From the Search dropdown list, select the type of setting you want to search for.
 - b. Enter part or all of a word in the setting you want to add and click **Find**.

 **Note:** If the search finds more than 500 values, no results appear. Use the preceding steps to refine your search criteria and show fewer results.
 - c. To add or remove columns, select one or more column names and click the **Add** or **Remove** arrow.
 - d. Use the **Top**, **Up**, **Down**, and **Bottom** arrows to arrange the columns in the sequence you want.
6. Click **Save**, or if you're cloning an existing view, rename it and click **Save As**.

Edit Multiple Permission Sets with Permission Set List Views

You can change permissions in up to 200 permission sets directly from the list view, without accessing individual permission set pages. Editable cells display a pencil icon () when you hover over the cell, while non-editable cells display a lock icon ()

 **Warning:** Use care when editing permission sets with this method. Because permission sets affect a user's access, making mass changes may have a widespread effect on users in your organization.

1. Select or create a list view that includes the permission sets and permissions you want to edit.
2. To edit multiple permission sets, select the checkbox next to each permission set you want to edit.

If you select permission sets on multiple pages, Salesforce remembers which permission sets are selected.
3. Double-click the permission you want to edit.

For multiple permission sets, double-click the permission in any of the selected permission sets.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To create, edit, and delete permission set list views:

- Manage Profiles and Permission Sets

To edit multiple permission sets from the list view:

- Manage Profiles and Permission Sets

AND

Customize Application

- In the dialog box that appears, enable or disable the permission.

In some cases, changing a permission may also change other permissions. For example, if “Customize Application” and “View Setup and Configuration” are disabled and you enable “Customize Application,” then “View Setup and Configuration” is also enabled. In this case, the dialog box lists the affected permissions.

- To change multiple permission sets, select **All n selected records** (where n is the number of permission sets you selected).
- Click **Save**.

If any errors occur, an error message appears, listing each permission set in error and a description of the error. Click the permission set name to open the permission set detail page. The permission sets you've clicked appear in the error window in gray, strike-through text. To view the error console, you must have pop-up blockers disabled for the Salesforce domain.

Any changes you make are recorded in the setup audit trail.

Search Permission Sets

To quickly navigate to other pages in a permission set, you can enter search terms in any permission set detail page.

On any of the permission sets detail pages, type at least three consecutive letters of an object, setting, or permission name in the  **Find Settings...** box. The search terms aren't case-sensitive. As you type, suggestions for results that match your search terms appear in a list. Click an item in the list to go to its settings page.

For some categories, you can search for the specific permission or setting name. For other categories, search for the category name.

Item	Search for	Example
Assigned apps	App name	Type <code>sales</code> in the Find Settings box, then select <code>Sales</code> from the list.
Objects	Object name	Let's say you have an Albums custom object. Type <code>album</code> , then select <code>Albums</code> .
<ul style="list-style-type: none"> Fields Record types 	Parent object name	Let's say your Albums object contains a Description field. To find the <code>Description</code> field for albums, type <code>album</code> , select <code>Albums</code> , and scroll down to <code>Description</code> under Field Permissions.
Tabs	Tab or parent object name	Type <code>rep</code> , then select <code>Reports</code> .
App and system permissions	Permission name	Type <code>api</code> , then select <code>API Enabled</code> .
All other categories	Category name	To find Apex class access settings, type <code>apex</code> , then select <code>Apex Class Access</code> . To find custom permissions, type <code>cust</code> , then select <code>Custom Permissions</code> . And so on.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To search permission sets:

- View Setup and Configuration

If you don't get any results, don't worry. Here's some tips that can help:

- Check if the search term has at least three consecutive characters that match the object, setting, or permission name.
- The permission, object, or setting you're searching for might not be available in the current Salesforce org.
- The item you're searching for might not be available for the user license that's associated with the current permission set. For example, a permission set with the Standard Platform User license doesn't include the "Modify All Data" permission.
- The permission set license associated with the permission set doesn't include the object, setting, or permission name you're searching for.

SEE ALSO:

[Permission Sets](#)

Report on Custom Permission Set and Permission Set Group Assignments

To help you manage users, report on your users' assigned custom permission set and permission set groups. Create a custom report type before building reports on custom permission set or permission set group assignments.

For example, see which users are assigned to each custom permission set or permission set group, or see an individual user's assignments.

[Create a Custom Report Type for Custom Permission Set and Permission Set Group Assignments](#)

Before you can build reports on custom permission set and permission set group assignments, create a custom report type.

[Build a Report on Custom Permission Set and Permission Set Group Assignments](#)

Report on your users' assignments to custom permission set and permission set groups.

Create a Custom Report Type for Custom Permission Set and Permission Set Group Assignments

Before you can build reports on custom permission set and permission set group assignments, create a custom report type.

 **Note:** This custom report type only applies for assignments for custom permission sets and permission set groups, not for standard permission sets and permission set groups.

1. From Setup, in the Quick Find box, enter *Report Types*, and then select **Report Types**.
2. Select **Permission Set Assignment** as the Primary Object.
3. Add a label and description.
4. Choose which category to store the report in.
5. Select a Deployment Status.
6. Click **Next**, and then save.
7. To customize which fields are displayed in the custom report type, in the Fields Available for Reports section, click **Edit Layout**. You can add fields related to the permission set and permission set group and any fields on the User object.
8. Save your work.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To create and update custom report types:

- Create and Customize Reports
- AND

Manage Custom Report Types

To create, edit, and delete reports:

- Create and Customize Reports
- AND

Manage Custom Report Types

To view reports on permission set or permission set group assignments:

- View Setup and Configuration

Build a Report on Custom Permission Set and Permission Set Group Assignments

Report on your users' assignments to custom permission set and permission set groups.

Here's how to configure a sample custom permission set or permission set group assignment report.

1. Create a new report. Select the custom report type created for custom permission set and permission set group assignments.
2. To see all records, adjust your filters so that Show Me is set to **All permission set assignments**.
3. Under Columns, select which fields to display.
4. Group rows to help with your analysis. For example, group by a custom permission set or permission set group name or ID to see all users who are assigned. You can also group by the user's name or ID to see which custom permission sets and permission set groups the user is assigned.
5. To help with your analysis, add charts for a visual overview of your data.

 **Note:** This report only shows assignments for custom permission sets and permission set groups. It doesn't show assignments for standard permission sets and permission set groups.

SEE ALSO:

[Create a Custom Report Type](#)

[Build a Report](#)

[Manage Permission Set Assignments](#)

[Assign Permission Set Groups to Users](#)

Object Reference for the Salesforce Platform: PermissionSetAssignment

Permission Set Groups

A permission set group streamlines permissions assignment and management. Use a permission set group to bundle permission sets together based on user job personas or roles.

Watch how you can assign permissions to users with permission set groups.

 [Watch a video](#)

Users assigned the permission set group receive the combined permissions of all the permission sets in the group. You can include a permission set in more than one permission set group. Updates in a permission set propagate to all permission set groups that include the permission set. You can also remove individual permissions from a group with the muting feature, to further customize the group.

 **Example:** Suppose that you have users in your sales department with these requirements.

- Use Sales Cloud Analytics templates and apps
- Create, edit, and delete surveys
- Read, create, edit, and delete accounts and opportunities
- Create and customize list views and reports

You have three permission sets that contain the permissions you need, plus other permissions.

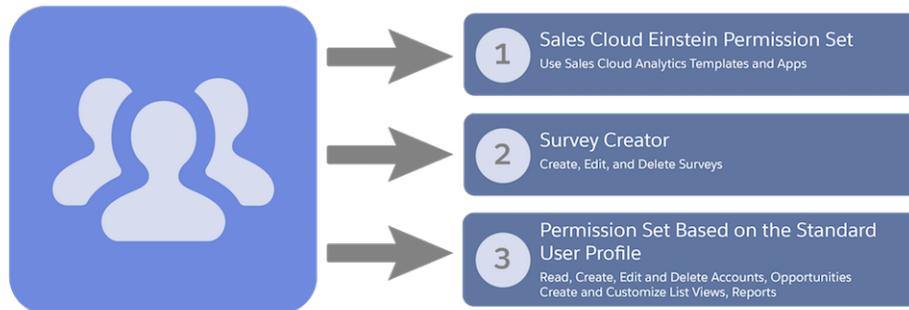
- Sales Cloud Einstein
- Survey Creator
- A permission set based on the Standard User Profile

EDITIONS

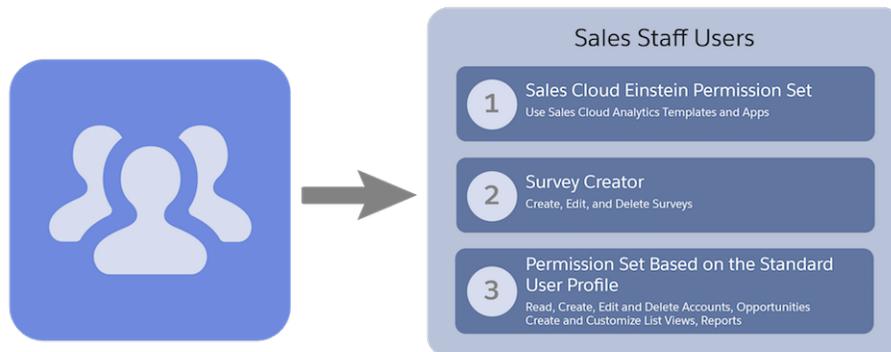
Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Essentials, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

Without permission set groups, you assign each permission set separately to this set of users.



With permission set groups, you create a single group based on the tasks that your sales employees regularly perform. You can call it Sales Staff Users. Then, assign the group to the sales employees. The permission set group contains the combined permissions of all three permission sets.



[Create a Permission Set Group](#)

Before you create a permission set group, assess your existing permission sets and users. Evaluate the types of job functions that your target group of users have, and group the permission sets based on their job functions.

[Assign Permission Set Groups to Users](#)

After you create a permission set group and add permission sets to it, assign the group to users.

[Muting Permission Sets](#)

Use a muting permission set with a permission set group to mute selected permissions. For instance, you have a subscriber org using a managed package that contains a permission set group. To use the existing permission set group, the subscriber org can disable permissions with a muting permission set.

[Permission Set Group Status and Recalculation](#)

A permission set group calculates the combined permissions from the included permission sets. The permission set group status indicates whether the calculation and resulting permissions in the group are up-to-date and available for the assigned users.

[Permission Set Groups from Managed Packages](#)

Partners can organize permissions into permission set groups to include in managed packages. Understand how to work with permission set groups installed from managed packages.

[Permission Set Groups Considerations](#)

When working with permission set groups, keep these behaviors in mind.

[Session-Based Permission Set Groups](#)

A session-based permission set group applies to a specific user session and grants users functional access to the permission sets included in the permission set group.

[Permission Set Groups and Combined Permissions View](#)

The Combined permissions section provides a centralized view of all the permissions included in permission sets that make up your permission set group.

[Permission Set Group FAQs](#)

Get answers to common questions about permission set groups.

Create a Permission Set Group

Before you create a permission set group, assess your existing permission sets and users. Evaluate the types of job functions that your target group of users have, and group the permission sets based on their job functions.

1. From Setup, in the Quick Find box, enter *Permission Set Groups*, then select **Permission Set Groups**.
2. Click **New Permission Set Group**.
3. Enter a label and description for the permission set group, and save your work.
4. To see your new permission set group in a list view, from Setup, select **Permission Set Groups** again, then from the list view dropdown menu choose **All Permission Set Groups**.

To delete a permission set group, select the permission set group in the list view to open the Permission Set Group detail page, then click **Delete**.

 **Note:** When you view permission set groups in a list view, **Delete** and other actions aren't available in the list view dropdown menu.

[Add Permission Sets to a Permission Set Group](#)

After you've created a permission set group, you can add permission sets to the group based on the needs of a particular user job role or persona. Create a customized view to filter the permission sets that can be added to a group.

[Remove Permission Sets from a Permission Set Group](#)

If you no longer need a permission set in a permission set group, you can remove the permission set from the group.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Essentials, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To create a permission set:

- Manage Profiles and Permission Sets

To assign a permission set:

- Assign Permission Sets

To create a permission set group:

- Manage Profiles and Permission Sets

Add Permission Sets to a Permission Set Group

After you've created a permission set group, you can add permission sets to the group based on the needs of a particular user job role or persona. Create a customized view to filter the permission sets that can be added to a group.

1. From Setup, in the Quick Find box, enter *Permission Set Groups*, and then select **Permission Set Groups**. Click the permission set group name in the list view.
2. In the Permission Set Group detail page, under Permission Sets, click **Permission Sets in Group**.
3. Click **Add Permission Set**. You can add up to 100 permission sets to a permission set group.
4. On the Add Permission Sets detail page, select the permission sets that you want to add to the group, and click **Add**.
5. Click **Done**. When the update is complete, the permission set group status changes to Updated.
6. To filter the list of permission sets that are available to be added to the group, on the Add Permission Sets detail page, click **Create New View**.
7. Specify options for view name, filter criteria, fields, and visibility, then click **Save**.
8. To open a customized view, select it from the View dropdown menu.

SEE ALSO:

[Permission Sets](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Essentials, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To create a permission set:

- [Manage Profiles and Permission Sets](#)

To assign a permission set:

- [Assign Permission Sets](#)

To create a permission set group:

- [Manage Profiles and Permission Sets](#)

Remove Permission Sets from a Permission Set Group

If you no longer need a permission set in a permission set group, you can remove the permission set from the group.

1. From Setup, in the Quick Find box, enter *Permission Set Groups*, and then select **Permission Set Groups**. Click the permission set group name in the list view.
2. In the Permission Set Group detail page, under Permission Sets, click **Permission Sets in Group**.
3. Select the permission sets that you want to remove from the group.
4. Click **Remove Permission Sets**.
5. Click **OK** to confirm the change, and click **Done**. When the update is complete, the permission set group status changes to Updated.

SEE ALSO:

[Permission Sets](#)

Assign Permission Set Groups to Users

After you create a permission set group and add permission sets to it, assign the group to users.

 **Important:** You can assign users only to permission set groups that have a status of Updated.

If permissions in the group require a permission set license, assign the permission set license to users before you assign the group to them. You can also assign permission set groups to a single user on the user's detail page in the Permission Set Group Assignments related list.

1. From Setup, in the Quick Find box, enter *Permission Set Groups*, and then select **Permission Set Groups**. Click the permission set group name in the list view.
2. Click **Manage Assignments** and then **Add Assignments**.
3. Select each user to whom you want to assign the group, and then click **Next**.
4. Optionally, select an expiration date for the user assignment to expire. For more information, see [Permission Set and Permission Set Group Assignment Expiration](#) in Salesforce Help.
5. Click **Assign**. When the update is complete, the permission set group status changes to Updated.

You can also remove permission set group assignments from the Manage Assignments page.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Essentials, Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To create a permission set:

- Manage Profiles and Permission Sets

To assign a permission set:

- Assign Permission Sets

To create a permission set group:

- Manage Profiles and Permission Sets

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Essentials, Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

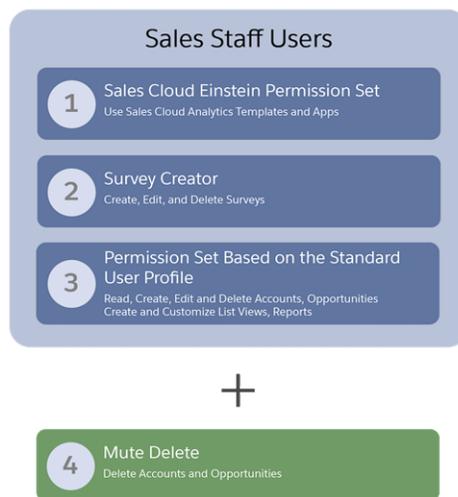
To assign permission sets:

- Assign Permission Sets

Muting Permission Sets

Use a muting permission set with a permission set group to mute selected permissions. For instance, you have a subscriber org using a managed package that contains a permission set group. To use the existing permission set group, the subscriber org can disable permissions with a muting permission set.

 **Example:** You have a permission set group called Sales Staff Users that contains three permission sets. One set enables Delete on Accounts and also on Opportunities, but you no longer want all group members to have the permissions. However, another permission set group also references this permission set.



Instead of creating another permission set, create a muting permission set. Mute Delete on Accounts and Opportunities, and assigned group users no longer have the permission for these objects. However, users assigned to the permission set outside of the group retain ability to delete on the objects. You can add up to one muting permission set per permission set group.



EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Essentials, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

[Mute a Permission in a Permission Set Group](#)

You can mute a single permission or several permissions in a permission set group. If you mute a permission in a permission set group, only the permission in the group is muted. Permissions within the permission sets aren't affected.

[Permission Set Group Muting Dependencies](#)

When you mute a permission in a permission set group, the muted permission impacts permissions that depend on it within the group. Understand how muting dependencies work and the effects of muting permissions on your users.

Mute a Permission in a Permission Set Group

You can mute a single permission or several permissions in a permission set group. If you mute a permission in a permission set group, only the permission in the group is muted. Permissions within the permission sets aren't affected.

Before muting permissions within a permission set group, review your business and user needs for the permission set group and understand how permission dependencies can affect users.

 **Note:** Muting only impacts group members. Users outside of the group who are assigned to permission sets remain unaffected.

1. From Setup, in the Quick Find box, enter *Permission Set Groups*, and then select **Permission Set Groups**.
2. Under API Name, select the permission set group in which you want to mute permissions.
3. Click **Muting Permission Set in Group** and then click **New**. Only one muting permission set is allowed per group.
4. Give your muting permission set a label and API name and click **Save**.
5. Click the link for your new muting permission set.
6. In Find Settings..., type the name of the object or permission that you want to update and click **Edit**.
7. Select **Muted** for the permission that you want to mute and click **Save**.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Essentials, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To mute a permission in a permission set group:

- Manage Profiles and Permission Sets

Accounts		
Object Permissions		
Permission Name	Enabled	Muted
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Create	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Edit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
View All	<input type="checkbox"/>	<input type="checkbox"/>
Modify All	<input type="checkbox"/>	<input checked="" type="checkbox"/>

8. A confirmation message displays. Review your changes and click **Save** or **Cancel**.

SEE ALSO:

[Permission Set Groups](#)

[Permission Set Group Muting Dependencies](#)

Permission Set Group Muting Dependencies

When you mute a permission in a permission set group, the muted permission impacts permissions that depend on it within the group. Understand how muting dependencies work and the effects of muting permissions on your users.

 **Note:** Users outside of the group whom you assign to the permission sets remain unaffected by muting. Your mutes only affect group members.

Muting permissions in a permission set group offers you granular control over user permission assignments, but keep in mind the impact on dependent permissions. The table contains examples of permission dependencies.

When you mute:	These permissions are also muted:
Read	Create, Edit, Delete, View All, and Modify All
Edit	Delete and Modify All Records
Delete	Modify All Records
View All	Modify All

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Essentials, Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

 **Example:** The Sales Staff Users permission set group contains three permission sets and a muting permission set. The muting permission set mutes Delete on Accounts and Opportunities.



 **Example:** When you mute Delete on an object, Modify All is automatically muted (even if you didn't enable it for that object). Modify All becomes disabled because it depends on full object access, which is no longer available when you mute Delete.

 Example:

Accounts

Object Permissions

Permission Name	Enabled	Muted
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Create	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Edit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
View All	<input type="checkbox"/>	<input type="checkbox"/>
Modify All	<input type="checkbox"/>	<input checked="" type="checkbox"/>

 **Example:** Similarly, if you mute Read on the object, then Create, Edit, Delete, View All, and Modify All are muted. If you can't read object data, then you can't perform actions such as delete on it.

 **Example:** Let's examine how the object changes that you make can affect a user permission. Say that one of the permission sets in your group enables the Activate Orders user permission. Because Activate Orders requires Edit and Read permissions on the Orders object, these object permissions are enabled when you enable Activate Orders.

However, let's say that users in the group no longer need Edit on the Orders object. When you mute Edit, notice that the permission set group no longer grants the Activate Orders user permission either, even though you didn't mute it. And, group users can no longer delete orders. Because both Activate Orders and Delete depend on Edit, these permissions are automatically muted.

SEE ALSO:

[Permission Set Groups](#)

[Mute a Permission in a Permission Set Group](#)

Permission Set Group Status and Recalculation

A permission set group calculates the combined permissions from the included permission sets. The permission set group status indicates whether the calculation and resulting permissions in the group are up-to-date and available for the assigned users.

Permissions in permission set groups are calculated immediately when you change a custom permission set contained in the permission set group. Whenever you add, delete, or edit a custom permission set in the group, a calculation is applied to ensure the correct aggregation of permissions. Permission changes for Salesforce-owned standard permission sets that are added to permission set groups are calculated daily.

Users assigned to the permission set group retain the combined permissions available in the group as of the last completed calculation.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Essentials, Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

You can also manually recalculate a permission set group. You can use a manual recalculation if your permission set group has a status of Failed after deployments or package updates. On the permission set group's detail page, click the **Recalculate** button.

Valid permission set group statuses and meanings:

STATUS	DESCRIPTION	User Assignment	Group Editing	Notes
Updated	Combined permissions correctly reflect all permissions added to the group.	Allowed	Allowed	
Outdated	Changes are captured and system is updating the permission set group.	Unable to modify user assignments for the group	Allowed	Users assigned to the group don't yet have the updated permissions.
Updating	The permission set group is recalculating because of recent changes to one or more of its permission sets. The recalculating process is quick, so you rarely see this status.	Not Allowed	Not Allowed	Users assigned to the group don't yet have the updated permissions. When the recalculation is complete, the group status changes to Updated or Failed.
Failed	The permission set group recalculation failed.	Not Allowed	Allowed	Verify if a recent addition of a component to one of the permission sets in the permission set group is causing the failure. Remove the recently added component and see if the error persists. If your permission set group references a managed package component, and the managed package gets into an inactive state, the permission set group fails recalculation. If you use managed packages, verify that they aren't expired. While a permission set group is in a failed state, changes aren't propagated to the combined permission page. Users assigned to the group don't have updated permissions.

Permission Set Groups from Managed Packages

Partners can organize permissions into permission set groups to include in managed packages. Understand how to work with permission set groups installed from managed packages.

Keep these considerations in mind when working with permission set groups installed from managed packages:

- To install or uninstall a package with permission set groups, a subscriber must have permission set groups enabled.
- Permission set groups installed from managed packages don't count against the maximum number of groups created. The limit on the number of created and installed permission set groups varies by edition.
- Certain Salesforce editions don't allow you to create or customize permission set groups. In these instances, permission set groups from managed packages can be installed and used.
- A permission set group installed from a managed package has the namespace of the package to avoid any naming collision with a local group that has the same name.
- To delete a permission set group from an installed managed package, first uninstall the package.
- You can add and delete local permission sets in permission set groups installed from a managed package.

Keep in mind that you can install a package with a permission set group and then add a muting permission set to it. Any permissions in the muting permission set disable those permissions for the group. Using a muting permission set with a packaged permission set group lets you easily customize permissions for a specific group of users and business needs.

Users outside of the permission set group who are assigned to the permission sets remain unaffected. And any permission sets in the group whose permissions are muted remain unaffected outside of the group.

Muting can be valuable with managed packages. Suppose you receive an automatic update from an ISV or Salesforce partner for a managed package you subscribe to. But you aren't ready to enable a new feature now made available by a managed permission set. You can still receive the update and its benefits while muting anything in permission set groups that you're not ready to adopt.

SEE ALSO:

[Permission Set Groups](#)

Permission Set Groups Considerations

When working with permission set groups, keep these behaviors in mind.

- You can add up to 100 permission sets to a permission set group.
- If your org has many permission sets, using permission set groups can help improve performance.
- When viewing permission set groups in a list view, no actions are available in the list view dropdown menu.
- If you include session-based permission sets in a permission set group, the permissions in them do not require session-based activation for users assigned to the group.
- When a permission set is part of a group, you can still assign the individual permission set, apart from the permission set group, to specified users as needed.
- If done during the deployment phase, an update to a permission set group triggers a recalculation. To test assignments, exclude changes to permission set groups in the deploy phase. Instead, add permission sets and user assignments to permission set groups in your test phase, which doesn't trigger a recalculation.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Essentials, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Essentials, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

- Permissions in permission set groups are calculated immediately when you change a custom permission set contained in the permission set group. Whenever you add, delete, or edit a custom permission set in the group, a calculation is applied to ensure the correct aggregation of permissions. Permission changes for Salesforce-owned standard permission sets that are added to permission set groups are calculated daily.

Session-Based Permission Set Groups

A session-based permission set group applies to a specific user session and grants users functional access to the permission sets included in the permission set group.

Let's say you have a Salesforce app that contains confidential information. You only want specific users to be able to access the information in this app during a specific session. Some users (for example, team managers) require expanded access for the same length of time. You can create a permission set group that includes the different permission sets required for the confidential access. To create custom logic for the expanded access, create a Flow or use the API. The session-based permission set group activates only when the manager-level users authenticate into your environment using a token. When the token expires, the users must reauthenticate to access the application again.

To activate session-based permission set groups via the API, provide a value for the `PermissionSetGroupId` field on the `SessionPermSetActivation` SOAP API object.

Before assigning session-based permission set groups to users, ensure that they can meet the conditions of the permission sets in the permission set group. For example, grant user access to the required tools, such as authenticators. As a best practice, inform users of the conditions under which they can access certain applications and tools.

-  **Important:** If you include a regular permission set in your session-based permission set group, the permission set group makes the permission set session-based. Users assigned to the permission set group have access to the permission set for the duration of the session. If a user is separately assigned permissions from a different permission set, those permissions remain effective for that user, even when the permission set group session ends. For example, you assign a session-based permission set group that contains View All Data. The user is assigned View All Data from a separate permission set outside the session-based permission set group. When the session ends for the permission set group, the user still has the View All Data permission from the regular permission set.

[Create Session-Based Permission Set Groups](#)

To allow users functional access to permission sets only during specified sessions, create a session-based permission set group. For example, grant access to an application only during an authenticated session. Then activate the session-based permission set group in a flow or via the API.

[Allow Users to Activate or Deactivate a Session-Based Permission Set Group](#)

Create a flow that users can run to activate or deactivate a session-based permission set group. The session-based permission set group grants users functional access to permission sets only during specified sessions.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Essentials, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

Create Session-Based Permission Set Groups

To allow users functional access to permission sets only during specified sessions, create a session-based permission set group. For example, grant access to an application only during an authenticated session. Then activate the session-based permission set group in a flow or via the API.

Before beginning, check out [Session-Based Permission Set Groups](#) to learn when to use them.

1. Create a permission set group and make sure to select **Session Activation Required**.
2. Assign permission sets to the permission set group.
If you include a regular permission set in your session-based permission set group, the permission set group makes the permission set session-based. Users assigned to the permission set group have access to the permission set for the duration of the session.
3. Assign the permission set group to users.
Before assigning session-based permission set groups to users, ensure that they can meet the conditions of the permission sets in the permission set group.

The session-based permission set group isn't in effect until a session is activated for it. To activate a session, provide a value for the `PermissionSetGroupId` field on the `SessionPermSetActivation` SOAP API. Or, you can create a flow that activates and deactivates the session-based permission set group.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Essentials, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To create permission sets:

- [Manage Profiles and Permission Sets](#)

To assign permission sets:

- [Assign Permission Sets](#)

To create a permission set group:

- [Manage Profiles and Permission Sets](#)

Allow Users to Activate or Deactivate a Session-Based Permission Set Group

Create a flow that users can run to activate or deactivate a session-based permission set group. The session-based permission set group grants users functional access to permission sets only during specified sessions.

Before beginning, check out [Session-Based Permission Set Groups](#) to learn when to use them.

 **Important:** You can run queries in flows that also activate session-based permission sets, however, don't make data or object updates those flows.

1. Create a session-based permission set group.
2. Create a flow in Flow Builder.
 - a. Use a Get Records element to look up the permission set group.
 - b. In the Get Records element, store the permission set group's name in a variable, so that you can use the name in the action.
 - c. Drag a Core Action element onto the canvas, and choose either **Activate Session-Based Permission Set** or **Deactivate Session-Based Permission Set**.
3. Activate your flow
4. Distribute your flow to the users who must run it.

 **Example:** Create a flow to pass a permission set group name to the **Activate Session-Based Permission Set** core action. First, add a **Get Records** element to your flow to look up the PermissionSetGroup object. Set the Name field to the name of your session-based permission set group. Then add the **Activate Session-Based Permission Set** core action, and set the input to your permission set group name.

 **Tip:** Make sure that users who want to run your flow have the Run Flows permission.

When the flow activates the session-based permission set group, the running user obtains access to the permissions specified in your permission set group during the current user session. If the flow deactivates the session-based permission set group, the permissions are no longer available to the user.

Permission Set Groups and Combined Permissions View

The Combined permissions section provides a centralized view of all the permissions included in permission sets that make up your permission set group.

Tracking permissions can be daunting, especially as permissions within permission groups expand and change due to permission dependencies or muting. The Combined Permission section is a great way to view permissions enabled in the group, drill down to view, and if necessary, take further action. You can analyze the permissions that are enabled for users assigned to the group and ensure security of the organization.

 **Note:** The Combined Permissions section doesn't reflect permissions that were muted or permission changes that don't have an updated status.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Essentials, Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To create permission sets:

- Manage Profiles and Permission Sets

To assign permission sets:

- Assign Permission Sets

To create a permission set group:

- Manage Profiles and Permission Sets

To open, edit, or create a flow in Flow Builder:

- Manage Flow

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Essentials, Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

Permission Set Group FAQs

Get answers to common questions about permission set groups.

[When Do I Use a Permission Set Group Instead of a Permission Set?](#)

Use a permission set group to bundle permission sets based on logical user groups and the tasks users perform.

[Can I Assign a User to a Permission Set Group That Has Permissions from a Permission Set License?](#)

Yes. Let's say you have a group that contains the Sales Cloud Einstein and the Survey Creator permission sets. Ensure that the users assigned to the group are also assigned the associated permission set licenses.

[Can I Include a Session-Based Permission Set in a Permission Set Group?](#)

Yes. However, because the assigned permission set group users receive the permissions in the session-based permission set, the users don't need a session to activate the permissions.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Essentials, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

When Do I Use a Permission Set Group Instead of a Permission Set?

Use a permission set group to bundle permission sets based on logical user groups and the tasks users perform.

For example, you can group three permission sets together for users in a sales org: Sales Cloud Einstein, Survey Creator, and a permission set based on the Standard User profile. Assign the single group to your users instead of the three different permission sets.

Partners can organize permissions into groups and include them in managed packages. Upgrade the package with updated permissions when needed. Partners can still allow subscriber administrators to extend the groups without creating more permission sets.

Can I Assign a User to a Permission Set Group That Has Permissions from a Permission Set License?

Yes. Let's say you have a group that contains the Sales Cloud Einstein and the Survey Creator permission sets. Ensure that the users assigned to the group are also assigned the associated permission set licenses.

If you try to assign a group to a user who doesn't have a license needed for the permissions in the group, you receive an assignment error.

Can I Include a Session-Based Permission Set in a Permission Set Group?

Yes. However, because the assigned permission set group users receive the permissions in the session-based permission set, the users don't need a session to activate the permissions.

You can continue to assign the session-based permission set to users outside of the group. These users still require session activation.

What Determines Field Access?

Several factors control whether users can view and edit specific fields in Salesforce. You can control users' access to fields at the record type, user, or field level.

- Page layouts—Set whether fields are visible, required, editable, or read only for a particular record type.
- Field-level security—Further restrict users' access to fields by setting whether those fields are visible, editable, or read only. These settings override field properties set in the page layout if the field-level security setting is more restrictive.
- Permissions—Some user permissions override both page layouts and field-level security settings. For example, users with the "Edit Read Only Fields" permission can always edit read-only fields regardless of any other settings.
- Universally required fields—Override field-level security or any less-restrictive settings on page layouts by making a custom field universally required.
- Lookup and system fields—If you enable the Require permission to view record names in lookup fields setting, you restrict who can view record names in lookup and system fields. Users must have Read access to these records or the View All Lookup Record Names permission to view this data.

After setting these items, confirm users' access to specific fields using the [field accessibility grid](#).

SEE ALSO:

[Modify Field Access Settings](#)

Verify Access for a Particular Field

See whether access to a field is restricted and at what level—record type, user profile, or field.

1. Navigate to the fields area of the appropriate object.
For Knowledge validation status picklists, from Setup, enter *Validation Statuses* in the **Quick Find** box, then select **Validation Statuses**.
2. Select a field and click **View Field Accessibility**.
3. Confirm that the field access is correct for different profiles and record types.
4. Hover over any field access setting to see whether the field is required, editable, hidden, or read only based on the page layout or field-level security.
5. Click any field access setting to change it.

To verify field accessibility by a specific profile, record type, or field, from Setup, enter *Field Accessibility* in the **Quick Find** box, then select **Field Accessibility**. From this page, choose a particular tab to view and then select whether you want to check access by profiles, record types, or fields.

 **Note:** In this user interface, you can't check access for permission sets.

SEE ALSO:

[What Determines Field Access?](#)

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

Page layouts are not available in **Database.com**

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To view field accessibility:

- Manage Profiles and Permission Sets

Modify Field Access Settings

From the field accessibility grid, you can change a field's accessibility in the page layout or in field-level security.

1. In Object Manager, select an object, and then click **Fields & Relationships**.
 2. Select a field and click **View Field Accessibility**.
 3. Select a field from the dropdown, and then click a cell in the table to change the field's accessibility.
 4. In the Field-Level Security section of the page, specify the field's access level for the profile.
 - If you want users to be able to read and edit the field, select **Visible**.
 - If you want users to be able to read but not edit the field, select **Visible** and **Read-Only**.
 - If you don't want users to be able to read or edit the field, make sure both options are deselected.
-  **Note:** We recommend that you use field-level security to control users' access to fields rather than creating multiple page layouts to control field access.
5. In the Page Layout section:
 - Select the **Remove or change editability** radio button and then change the field access properties for the page layout. These changes will affect all profile and record type combinations that currently use this page layout.
 - Alternatively, you can select the **Choose a different page layout** radio button to assign a different page layout to the profile and record type combination.

SEE ALSO:

[What Determines Field Access?](#)

Field-Level Security

Field-level security settings let you restrict users' access to view and edit specific fields.

Watch how you can restrict access to specific fields using permission sets.

 [Watch a video](#)

Your Salesforce org contains lots of data, but you probably don't want every field accessible to everyone. For example, your payroll manager probably wants to keep salary fields accessible only to select employees. You can restrict user access in:

- Detail and edit pages
- Related lists
- List views
- Reports
- Connect Offline
- Email and mail merge templates
- Custom links
- The partner portal

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To view field accessibility:

- Manage Profiles and Permission Sets

To change field accessibility:

- Customize Application AND Manage Profiles and Permission Sets

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

- The Salesforce Customer Portal
- Synchronized data
- Imported data

Page layouts and field-level security settings determine which fields a user sees. The most restrictive field access settings of the two always applies. For example, you can have a field that's required in a page layout but is read-only in the field-level security settings. The field-level security overrides the page layout, so the field remains read-only.

You can define field-level security in either of these ways.

- [For multiple fields on a single permission set or profile](#)
- [For a single field on all permission sets](#)
- [For a single field on all profiles](#)

After setting field-level security, you can:

- Organize the fields on detail and edit pages by creating page layouts.



Tip: Use field-level security to restrict users' access to fields, and then use page layouts to organize detail and edit pages within tabs. This approach reduces the number of page layouts for you to maintain.

- Verify users' access to fields by checking field accessibility.
- Customize search layouts to set the fields that appear in search results, in lookup dialog search results, and in the key lists on tab home pages. To hide a field that's not protected by field-level security, omit it from the layout.



Note: Roll-up summary and formula fields are read-only on detail pages and not available on edit pages. They can also be visible to users even though they reference fields that your users can't see. Einstein Insights can also be visible to the user even though the insight references fields that your users can't see. Universally required fields appear on edit pages regardless of field-level security.

The relationship group wizard allows you to create and edit relationship groups regardless of field-level security.

Set Field Permissions in Permission Sets and Profiles

Field permissions specify the access level for each field in an object.

1. From Setup, enter *Permission Sets* in the **Quick Find** box, then select **Permission Sets**, or enter *Profiles* in the **Quick Find** box, then select **Profiles**.
2. Select a permission set or profile.
3. Depending on which interface you're using, do one of the following:
 - Permission sets or enhanced profile user interface—In the **Find Settings...** box, enter the name of the object you want and select it from the list. Click **Edit**, then scroll to the Field Permissions section.
 - Original profile user interface—In the Field-Level Security section, click **View** next to the object you want to modify, and then click **Edit**.
4. Specify the field's access level.
5. Click **Save**.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To set field-level security:

- Manage Profiles and Permission Sets
- AND
- Customize Application

Set Field-Level Security for a Field on All Profiles

Use the object manager to set field-level security settings on profiles.

1. From Setup, open **Object Manager**, and then in the Quick Find box, enter the name of the object containing the field.
2. Select the object, and then click **Fields & Relationships**.
3. Select the field you want to modify.
4. Click **Set Field-Level Security**.
5. Specify the field's access level.
6. Save your changes.

Set Field-Level Security for a Field on All Permission Sets

Set field-level security for a field on permission sets. This option is an alternative to setting field-level security for a field on profiles.

1. From Setup, in the Quick Find box, enter *User Management Settings*, and then select **User Management Settings**. Enable **Field-Level Security for Permission Sets during Field Creation** if it isn't already enabled.
2. In Object Manager, select an object, and then click **Fields & Relationships**.
3. Select the field that you want to modify.
4. Click **Set Field-Level Security**.
5. Specify the field's access level. You can only set field-level security in custom permission sets created for your org.
 -  **Note:** Select **Permission sets with object permissions** to filter the list to permission sets that have Create, Read, Edit, or Delete access on the field's object. Deselect this option to show all permission sets. If no permission sets have object permissions for the field's object, the list contains all permission sets.
6. Save your changes.

SEE ALSO:

[Enable Field-Level Security for Permission Sets during Field Creation](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To set field-level security:

- Manage Profiles and Permission Sets
- AND
- Customize Application

EDITIONS

Available in: **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To set field-level security:

- Manage Profiles and Permission Sets
- AND
- Customize Application

What Is a Group?

A group consists of a set of users. A group can contain individual users, other groups, or the users in a particular role or territory. It can also contain the users in a particular role or territory plus all the users below that role or territory in the hierarchy.

There are two types of groups.

- **Public groups**—Administrators and delegated administrators can create public groups. Everyone in the organization can use public groups. For example, an administrator can create a group for an employee carpool program. All employees can then use this group to share records about the program.
- **Personal groups**—Each user can create groups for their personal use. For example, users might need to ensure that certain records are always shared within a specified workgroup.

 **Tip:** Permission set groups consist of permission sets rather than users. Permission set groups bundle permission sets based on job functions or tasks. To learn more about permission set groups and why you use them, see [Permission Set Groups](#).

You can use groups in the following ways.

- To set up default sharing access via a sharing rule
- To share your records with other users
- To specify that you want to synchronize contacts owned by other users
- To add multiple users to a Salesforce CRM Content library
- To assign users to specific actions in Salesforce Knowledge

Public Group Considerations

For organizations with a large number of users, consider these tips when creating public groups to optimize performance.

Group Member Types

Many types of groups are available for various internal and external users.

Create and Edit Groups

Only administrators and delegated administrators can create and edit public groups, but anyone can create and edit their own personal groups in Salesforce Classic. Personal groups aren't available in Lightning.

View Group Lists

View and edit information about a group and its members.

Monitor Public Group Members with Reports

See all users, roles, roles, territories, and other groups. Create a custom report type before building reports on public group members.

Sharing Records with Manager Groups

Share records up or down the management chain using sharing rules or manual sharing.

EDITIONS

Available in: both Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

Public Group Considerations

For organizations with a large number of users, consider these tips when creating public groups to optimize performance.

- Create a group when at least a few users need the same access.
- Create a group for members who don't need to frequently move in or out of the groups.
- If your group contains more than 10,000 members, for improved performance, adjust group membership using the GroupMember API object instead of the group's detail page in Setup.
- Avoid creating groups within groups that result in more than five levels of nesting.
- Enable automatic access to records using role hierarchies for public groups by selecting **Grant Access Using Hierarchies** when creating the group. However, don't use this option if you're creating a public group with All Internal Users as members.
- After enabling digital experiences, all Roles and Subordinates members in groups are converted to Roles, Internal and Portal Subordinates members. Review public groups that contain Roles, Internal and Portal Subordinates members, and replace them with Role and Internal Subordinates as required.

SEE ALSO:

[What Is a Group?](#)

Group Member Types

Many types of groups are available for various internal and external users.

When you create or edit a group, you can select the following types of members from the `Search` drop-down list. Depending on your organization settings, some types may not be available.

Member Type	Description
Customer Portal Users	All of your Customer Portal users. This is only available when a customer site or portal is enabled for your organization.
Partner Users	All of your partner users. This is only available when a partner site or portal is enabled for your organization.
Personal Groups	All of your own groups. This is only available when creating other personal groups.
Portal Roles	All roles defined for your organization's site or portal. This includes all users in the specified role, except high-volume users. A site or portal role name includes the name of the account that it's associated with, except for person accounts, which include the user Alias .
Portal Roles and Subordinates	All roles defined for your organization's site or portal. This includes all of the users in the

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

The member types that are available vary depending on your edition.

USER PERMISSIONS

To create or edit a public group:

- Manage Users

To create or edit another user's personal group:

- Manage Users

Member Type	Description
	<p>specified role plus all of the users below that role in the site or portal role hierarchy, except for high-volume users.</p> <p>A site or portal role name includes the name of the account that it's associated with, except for person accounts, which include the user Alias.</p>
Public Groups	All public groups defined by your administrator.
Roles	All roles defined for your organization. Adding a role to a group includes all of the users in that role, but does not include site or portal roles.
Roles and Internal Subordinates	Adding a role and its subordinate roles includes all of the users in that role plus all of the users in roles below that role. This doesn't include site or portal roles or users.
Roles and Subordinates	<p>Adding a role and its subordinate roles includes all of the users in that role plus all of the users in roles below that role. This is only available when no Salesforce Experience sites or portals are enabled for your organization.</p> <p> Warning: After enabling digital experiences, all Roles and Subordinates members in groups are converted to Roles, Internal and Portal Subordinates members. Review public groups that contain Roles, Internal and Portal Subordinates members, and replace them with Role and Internal Subordinates as required.</p>
Roles, Internal and Portal Subordinates	Adding a role and its subordinate roles includes all of the users in that role plus all of the users in roles below that role. This is only available when Salesforce Experiences or portals are enabled for your organization. This includes site and portal users.
Users	All users in your organization. This doesn't include site or portal users.

 **Note:** You can't add unauthenticated guest users to public groups.

SEE ALSO:

[What Is a Group?](#)

[Sharing Records with Manager Groups](#)

Create and Edit Groups

Only administrators and delegated administrators can create and edit public groups, but anyone can create and edit their own personal groups in Salesforce Classic. Personal groups aren't available in Lightning.

 **Note:** When you edit groups, roles, and territories, sharing rules are recalculated to add or remove access as needed.

Depending on the nature of your updates and your org's setup, these sharing calculations can take a while to complete. If you experience sharing evaluations or timeouts, consider deferring sharing calculations before making large-scale updates, and then restart and recalculate sharing at a later time. For more information, see [Defer Sharing Calculations](#) in Salesforce Help.

To create or edit a group:

- Click the control that matches the type of group:
 - For personal groups, go to your personal settings in Salesforce Classic and click **My Personal Information** or **Personal**—whichever one appears. Then click **My Groups**. The Personal Groups related list is also available on the user detail page.
 - For public groups, from Setup, in the Quick Find box, enter *Public Groups*, then select **Public Groups**.
- Click **New**, or click **Edit** next to the group you want to edit.
- For Label, enter the name used to refer to the group in any user interface pages.
- For public groups, enter the unique Group Name used by the API and managed packages.
- To allow automatic access to records using your role hierarchies, select **Grant Access Using Hierarchies**. When selected, any records shared with users in this group are also shared with users higher in the hierarchy. Deselect **Grant Access Using Hierarchies** if you're creating a public group with All Internal Users as members, which optimizes performance for sharing records with groups.

 **Note:** If **Grant Access Using Hierarchies** is deselected, users that are higher in the role hierarchy don't receive automatic access. However, some users can still access records they don't own. Examples of such users include users with the View All and Modify All object permissions and the View All Data and Modify All Data system permissions.
- From the Search dropdown, select the type of member to add. If you don't see the member you want to add, enter keywords in the search box and click **Find**.

 **Note:** For account owners to see child records owned by high-volume Experience Cloud site users, they must be members of any share groups with access to the site users' data.
- Select members from the Available Members box, and click **Add** to add them to the group.

If your group contains more than 10,000 members, for improved performance, adjust group membership using the GroupMember API object instead of the group's detail page in Setup.
- For public groups, specify any delegated administration groups whose members can add or remove members from this public group. Select groups from the Available Delegated Groups box, and then click **Add**.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience (except personal groups)

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To create or edit a public group:

- Manage Users

To create or edit another user's personal group:

- Manage Users

9. Save your changes.

SEE ALSO:

[What Is a Group?](#)

View Group Lists

View and edit information about a group and its members.

1. Click the control that matches the type of group.
 - For personal groups, in your personal settings, click **My Personal Information** or **Personal**—whichever one appears. Then click **My Groups**.
 - For public groups, from Setup, in the Quick Find box, enter *Public Groups*, then select **Public Groups**.
2. To display the group's detail page, click the name of a group in the Groups related list.
 - To edit the group membership, click **Edit**.
 - To delete the group, click **Delete**.
 - To view active group members, see the Group Members related list.
 - To view all group members and users who have equivalent access because they're higher in the role or territory hierarchy, click **View All Users**. From the All Users in Group related list you can view detailed user information, edit user information, and access-related information.

You can also view the public groups that a user is a member of. From Setup, in the Quick Find box, enter *Users*, then select **Users** and select the user. In the Public Group Membership related list, you can:

- To create a public group, click **New Group**.
- Click a public group name to view its details.

SEE ALSO:

[What Is a Group?](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To edit a public group:

- Manage Users

Monitor Public Group Members with Reports

See all users, roles, roles, territories, and other groups. Create a custom report type before building reports on public group members.

[Create a Custom Report Type for Public Group Members](#)

Before you can build reports on public group members, create a custom report type.

[Report on Public Group Membership](#)

Build a report on public group members. Public group members can be users, roles, territories, and other public groups.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To create and update custom report types:

- Create and Customize Reports
- AND
- Manage Custom Report Types

To create, edit, and delete reports:

- Create and Customize Reports
- AND
- Manage Custom Report Types

To view members of all public groups:

- Manage Users

Create a Custom Report Type for Public Group Members

Before you can build reports on public group members, create a custom report type.

1. From Setup, in the Quick Find box, enter *Report Types*, and then select **Report Types**.
2. Select **Group Member** as the Primary Object.
3. Add a label and description.
4. Choose which category to store the report in.
5. Select a Deployment Status.
6. Click **Next**, and then save.
7. To customize which fields are displayed in the custom report type, in the Fields Available for Reports section, click **Edit Layout**. To add fields, click **Add fields related via lookup**, and then select any of these supported fields: Group ID, Group Name, Group Type, Included Group ID, Included Group Name, Included Group Type, User ID, User Full Name, User Active, User Type, and User Email. Click **OK**, and then click **Save**.
8. Save your work.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To create and update custom report types:

- Create and Customize Reports
- AND
- Manage Custom Report Types

To view members of all public groups:

- Manage Users

Report on Public Group Membership

Build a report on public group members. Public group members can be users, roles, territories, and other public groups.

Here's how to configure a sample public group members report.

1. Create a new report. Select the custom report type created for group members.
2. To see all public group members, adjust your filters so that Show Me is set to **All group member** and **Created Date** is set to All Time.
3. Under Columns, select which fields to display.
4. To see only members of public groups and filter out other types of groups, add a filter for Group: Type so that the field's value must equal Regular. There are multiple values available for Group: Type, but only Regular and Queue are supported.
5. Group rows to help with your analysis. For example, group by the public group's name or ID to see which users or other included groups are members. You can also group by the member's name or ID to see which public group they're added to.
6. To help with your analysis, add charts for a visual overview of your data.

 **Note:** For public groups containing all users in a specified role, the report displays the role sharing group ID in the Included Group: Group ID field. The role ID isn't displayed. For more information, see [Role and Territory Sharing Groups](#) in Salesforce Help.

SEE ALSO:

[Create a Custom Report Type](#)

[Build a Report](#)

[Object Reference for the Salesforce Platform: GroupMember](#)

Sharing Records with Manager Groups

Share records up or down the management chain using sharing rules or manual sharing.

The role hierarchy controls the level of visibility that users have into your organization's data. You can use manager groups to share records with your management chain, instead of all managers in the same role based on the role hierarchy. Manager groups can be used wherever other groups are used, such as in a manual share or sharing rule. But they can't be added to other groups and don't include site or portal users. Manager groups can contain Standard and Chatter Only users only.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To create, edit, and delete reports:

- Create and Customize Reports

AND

Manage Custom Report Types

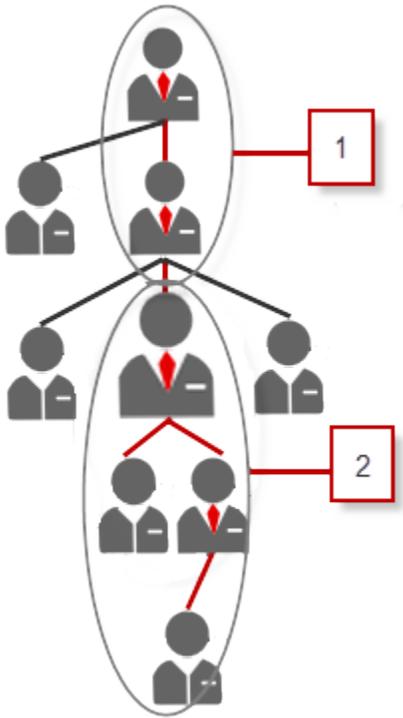
To view members of all public groups:

- Manage Users

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions



Every user has two manager groups—Managers Group (1) and Manager Subordinates Group (2)—where Managers Group includes a user’s direct and indirect managers, and Manager Subordinates Group includes a user and the user’s direct and indirect reports. On a sharing rule Setup page, these groups are available on the Share with dropdown list.

To find out who a user’s manager is, from Setup, in the Quick Find box, enter *users*, then select **Users**. Click a user’s name. The **Manager** field on the user detail page displays the user’s manager.

To enable users to share records with the manager groups, follow these steps.

1. From Setup, in the Quick Find box, enter *Sharing Settings*, then select **Sharing Settings**.
2. On the Sharing Settings page, click **Edit**.
3. In Other Settings, select **Manager Groups** and then click **Save**.

 **Note:** You can’t disable manager groups if your organization uses WDC or has any sharing rules that use manager groups.

With manager groups, you can share records to these groups via manual sharing, sharing rules, and Apex managed sharing. Apex sharing reasons isn’t supported. For Apex managed sharing, include the row cause ID, record ID, and the manager group ID. For more information, see the [Lightning Platform Apex Code Developer’s Guide](#).

Inactive users remain in the groups of which they’re members, but all relevant sharing rules and manual sharing are retained in the groups.

 **Note:** If your organization has User Sharing enabled, you can’t see the users whom you don’t have access to. Additionally, a querying user who doesn’t have access to another user can’t query that user’s groups.

 **Example:** You might have a custom object for performance reviews whose organization-wide default is set to Private. After deselecting the **Grant Access Using Hierarchies** checkbox, only the employee who owns the review record can

view and edit it. To share the reviews up the management chain, administrators can create a sharing rule that shares to a user's Managers Group. Alternatively, the employee can share the review record with the user's Managers Group by using manual sharing.

SEE ALSO:

[Sharing Settings](#)

[Sharing Rules](#)

[Sharing Rule Categories](#)

Sharing Settings

In Salesforce, you can control access to data at many different levels. For example, you can control the access your users have to objects with object permissions. Within objects, you can control the access users have to fields using field-level security. To control access to data at the record level, use sharing settings and restriction rules.

 **Note:**  [Who Sees What: Overview \(English only\)](#)

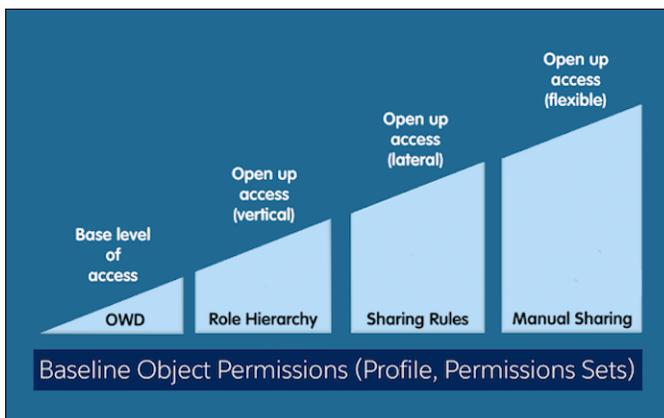
Watch how you can control who sees what data in your organization.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

Teams are not available in **Database.com**



There are several sharing mechanisms that you can use to configure record access for your users.

Organization-Wide Defaults

Your organization-wide default sharing settings give you a baseline level of access for each object. Organization-wide sharing settings specify the default level of access that users have to each others' records. For example, you can set the organization-wide default for leads to Private if you only want users to view and edit the leads they own. Then, you can create lead sharing rules to extend access of leads to particular users or groups.

Role Hierarchy

The role hierarchy automatically grants record access to users above the record owner in the hierarchy. You can control sharing access using hierarchies for any custom object, but not standard objects.

Sharing Rules

Sharing rules represent the exceptions to your organization-wide default settings. They allow you to extend record access to users regardless of their place in the role hierarchy. If you have organization-wide sharing defaults of Public Read Only or Private, you can define rules that give additional users access to records they don't own. You can create sharing rules based on record owner or field values in the record.

Manual Sharing

Sometimes it's impossible to define a consistent group of users who need access to a particular set of records. Record owners can use manual sharing to give read and edit permissions to users who don't have access any other way. Manual sharing isn't automated like organization-wide sharing settings, role hierarchies, or sharing rules. But it gives record owners the flexibility to share records with users that must see them.

Apex Managed Sharing

Apex managed sharing allows developers to programmatically share custom objects. When you use Apex managed sharing to share a custom object, only users with the "Modify All Data" permission can add or change the sharing on the custom object's record, and the sharing access is maintained across record owner changes.

Other Methods for Controlling Access to Records

In addition to sharing settings, there are a few other ways to allow multiple users access to given records, or to filter records so users don't have too much access.

Map category groups to roles

Control access to data categories by mapping them to user roles.

Queues

Queues help you prioritize, distribute, and assign records to teams who share workloads. Queue members and users higher in a role hierarchy can access queues from list views and take ownership of records in a queue.

Use queues to route lead, order, case, and custom object records to a group.

Teams

For accounts, opportunities, and cases, record owners can use teams to allow other users access to their records. A *team* is a group of users that work together on an account, sales opportunity, or case. Record owners can build a team for each record that they own. The record owner adds team members and specifies the level of access each team member has to the record, so that some team members can have read-only access and others can have read/write access. The record owner can also specify a role for each team member, such as "Executive Sponsor." In account teams, team members also have access to any contacts, opportunities, and cases associated with an account.



Note: A team member can have a higher level of access to a record for other reasons, such as a role or sharing rule. In this case, the team member has the highest access level granted, regardless of the access level specified in the team.

Restriction Rules

When a restriction rule is applied to a user, the data that they had read access to via your sharing settings is further scoped to only records matching the record criteria that you set. This behavior is similar to how you can filter results in a list view or report, except that it's permanent.

[Manage Sharing Settings](#)

Use the Sharing Settings page to manage your organization-wide sharing defaults, sharing rules, and other sharing settings.

[Considerations for Making Sharing Updates](#)

Review these considerations before making sharing changes, such as updates to organization-wide defaults, sharing rules, account ownerships, or group memberships.

[Manual Sharing](#)

Manual sharing gives other users access to certain types of records, including accounts, contacts, and leads.

[Viewing Which Users Have Access to Your Records in Salesforce Classic](#)

When viewing a record, you can view a list of users who have been granted access through sharing. The list includes their access level and an explanation and shows every user who has access that's greater than the org-wide default settings.

[Viewing Which Users Have Access to Your Records in Lightning Experience](#)

When viewing a record, you can view a list of users who have been granted access to the record through sharing. The list includes their access level and an explanation and shows every user who has access that's greater than the org-wide default settings.

[See Account Access from Manual Shares or Account Teams with Reports](#)

See the account records that are shared manually or through account teams in your Salesforce org and which users or groups have access to them. Before building reports, create a custom report type on the Account Share object, which represents sharing entries on an account.

[Manage Additional Sharing Settings](#)

Besides configuring the organization-wide defaults and sharing rules, you can configure the following items on the Sharing Settings Setup page.

[Object-Specific Share Locks](#)

When you create, edit, or delete a sharing rule, recalculation runs to update record access in your Salesforce org. This operation can take some time if you have many users and records. The object-specific share locks feature enables you to make changes to a sharing rule for other objects simultaneously, depending on the objects affected by the sharing rules, sharing rule type, and target groups or roles of the affected users.

SEE ALSO:[Organization-Wide Sharing Defaults](#)[Sharing Rules](#)[Create a User Role](#)[Sharing Considerations](#)[Restriction Rules](#)

Manage Sharing Settings

Use the Sharing Settings page to manage your organization-wide sharing defaults, sharing rules, and other sharing settings.

To view the sharing settings page, from Setup, in the Quick Find box, enter *Sharing Settings*, and then select **Sharing Settings**.

- From the `Manage sharing settings for` dropdown list, select All Objects to view sharing settings for all objects in the organization, or select a single object.
- [View or manage organization-wide defaults, or the default level of access users have to each other's records.](#)
- [View or manage sharing rules, or exceptions to the organization-wide defaults.](#)
- [View the profiles that override sharing settings.](#)
- [Manage other sharing settings, such as enabling report visibility, manual user record sharing, and manager groups.](#)

Sharing Considerations

Learn how sharing models give users access to records they don't own.

The sharing model is a complex relationship between role hierarchies, user permissions, sharing rules, and exceptions for certain situations. Review the following notes before setting your sharing model. For considerations on sharing rules specifically, see [Sharing Rule Considerations](#).

Exceptions to Role Hierarchy-Based Sharing

Users can always view and edit all data owned by or shared with users below them in the role hierarchy. Exceptions to role hierarchy sharing include:

- Disabling the Grant Access Using Hierarchies setting in your organization-wide default settings allows you to ignore the hierarchies when determining access to data. You can only modify this setting for custom objects.
- Contacts that aren't linked to an account are always private. Only the owner of the contact and administrators can view it. Contact sharing rules don't apply to private contacts.
- Notes and attachments marked as private via the `Private` checkbox are accessible only to the person who attached them and to administrators.
- Events marked as private via the `Private` checkbox are accessible only by the event owner. Other users can't see the event details when viewing the event owner's calendar. However, users with the "View All Data" or "Modify All Data" permission can see private event details in reports and searches, or when viewing other users' calendars.
- Users above a record owner in the role hierarchy can only view or edit the record owner's records if they have the "Read" or "Edit" object permission for the type of record.
- Visibility to users as a result of the Site User Visibility preference isn't inherited through the role hierarchy. If a manager in the role hierarchy isn't a member of a site, but their subordinate is, the manager doesn't gain access to other members of the site. This only applies if Salesforce Experiences are enabled in your organization.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Starter, Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To set default sharing access:

- [Manage Sharing](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited,** and **Developer** editions

Deleting Records

- The ability to delete individual records is controlled by administrators, the record owner, users in a role hierarchy above the record owner, and any user who has been granted “Full Access.”
- If the org-wide default is set to Public Read/Write/Transfer for cases or leads, only the record owner or administrator can delete the record.

Adding Related Items to a Record

- You must have “Read/Write” access to a record to be able to add notes or attachments to the record.
- You must have at least “Read” access to a record to be able to add activities or other associated records to it.

Adding or Removing Sharing Access Manually

- The ability to manually extend the sharing access of individual records is controlled by administrators, the record owner, users in a role hierarchy above the record owner, and any user that has been granted “Full Access.”
- If you’re manually sharing an opportunity, contact, or case, the users you share it with must have at least Read access to the associated parent account via sharing features or you must have the ability to also share the account. You have the ability to share the account if you are the account owner, are a system administrator, are above the account owner in the role hierarchy, and or have the Modify All permission on accounts. If you have the ability to share the account itself, the users you share the opportunity, contact, or case with are automatically given Read access to the parent account.
- If a user transfers ownership of a record, Salesforce deletes any manual shares created by the original record owner, which can cause users to lose access. When account ownership is transferred, manual shares created by the original account owner on child records, such as opportunities and cases, are also deleted.

Changing Record Owners

- To transfer ownership of a case, contact, or opportunity record, either:
 - The new owner must already have at least read access to its associated parent account via sharing features.
 - The user who is transferring the record must have the ability to share the associated parent account. The account owner, system administrators, users who are above the account owner in the role hierarchy, and users with the Modify All permission on account have this ability.

Otherwise, the ownership transfer can’t be completed.

User Permissions and Object-Level Permissions

While your sharing model controls visibility to records, user permissions and object-level permissions control what users can do to those records.

- Regardless of the sharing settings, users must have the appropriate object-level permissions. For example, if you share an account, those users can only see the account if they have the “Read” permission on accounts. Likewise, users who have the “Edit” permission on contacts aren’t able to edit contacts they don’t own if they’re working in a Private sharing model.
- Administrators, and users with the “View All Data” or “Modify All Data” permissions, have access to view or edit all data.

Account Sharing

- To restrict users' access to records they don’t own that are associated with accounts they do own, set the appropriate access level on the role. For example, you can restrict a user's access to opportunities they don’t own yet are associated with accounts they do own using the `Opportunity Access` option.

Apex Sharing

The organization-wide default settings can't be changed from private to public for a custom object if Apex code uses the sharing entries associated with that object. For example, if Apex code retrieves the users and groups who have sharing access on a custom object `Invoice__c` (represented as `Invoice__share` in the code), you can't change the object's organization-wide sharing setting from private to public.

Campaign Sharing

- In Professional, Enterprise, Unlimited, Performance, and Developer Editions, designate all users as Marketing Users when enabling campaign sharing. This designation simplifies administration and troubleshooting because access can be controlled using sharing and profiles.
- To segment visibility between business units while maintaining existing behavior within a business unit, set the campaign organization-wide default to Private. Create a sharing rule to grant marketing users Public Full Access to all campaigns owned by users within their business unit. Then create a sharing rule to grant all non-marketing users in a business unit Read Only access to all campaigns owned by users in their business unit.
- When a single user, such as a regional marketing manager, owns multiple campaigns and must segment visibility between business units, share campaigns individually instead of using sharing rules. Sharing rules apply to all campaigns owned by a user and don't allow segmenting visibility.
- Create all campaign sharing rules before changing your organization-wide default to reduce the effect the change has on your users.
- To share all campaigns in your organization with a group of users or a specific role, create a sharing rule that applies to campaigns owned by members of the "Entire Organization" public group.
- Minimize the number of sharing rules by using the "Roles and Subordinates" option instead of choosing a specific role.
- If campaign hierarchy statistics are added to the page layout, a user can see aggregate data for a parent campaign and all the campaigns below it in the hierarchy regardless of whether that user has sharing rights to a particular campaign within the hierarchy. Therefore, consider your organization's campaign sharing settings when enabling campaign hierarchy statistics. If you don't want users to see aggregate hierarchy data, remove any or all of the campaign hierarchy statistics fields from the Campaign Hierarchy related list. These fields are still available for reporting purposes.
- If the sharing model is set to Public Full Access for campaigns, any user can delete those types of records.

Campaign Member Sharing

Campaign member sharing is controlled by campaign sharing rules. Users that can see a campaign can also see associated campaign members.

Contact Sharing

See: [Business Contact Sharing for Orgs That Use Person Accounts](#)

Price Book Sharing

- Sharing on price books controls whether users can add the price book and its products to opportunities.

- User permissions control whether users can view, create, edit, and delete price books.

SEE ALSO:

[Sharing Rules](#)

[Sharing Settings](#)

[Customize Who Has Access to Paused Flow Interviews](#)

Who Has Access to Account Records?

Different sharing mechanisms can grant a user access to an account.

A user can have access to an account from:

- Record ownership
- Implicit access from an associated child record such as a case, contact, or opportunity
- Organization-wide sharing defaults
- Role hierarchy
- Sharing rules
- Manual sharing
- Account team or territory

To find out why a user has access to the record, in Lightning Experience, click **Sharing Hierarchy**

from the Action Menu on the account record. Click **View** next to the user's name. In Salesforce Classic, click **Sharing** on the account detail page, then click **Expand List** to see all users who have access. Click **Why?** next to the user's name.

These users don't show up in the list even if they have access.

- All users, if the organization-wide defaults are set to Public Read Only or Public Read/Write
- High-volume Experience Cloud site users

 **Note:** If the **Sharing Hierarchy** or **Sharing** buttons don't appear, the organization-wide sharing defaults are likely set to Controlled by Parent or Public Read. Otherwise, only the record owner, an administrator, or a user above the owner in the role hierarchy can see the Sharing Detail page.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** editions

Table 4: Troubleshooting guideline for user access to a record

Access Type	Description
Record owner	Record owners always get access to their own records.
Implicit access	Corresponds to the "Associated record owner or sharing" entry in the Reason column of the Sharing Detail page. The user has access to a child record of an account (opportunity, case, or contact), which grants them Read access on that account. You can't overwrite this access. For example, if the user has access to a case record, he or she has implicit Read access to the parent account record.
Organization-wide sharing default	Check if the defaults for the account object are set to Private. If it is, the user has gained access via other methods listed here. It must be set to Private if at least one of your users must not see a record.
Role hierarchy	The user inherited Read access from a subordinate in the role hierarchy. You can't override this behavior for non-custom objects. If the user who has access is on a different branch of the hierarchy from the account owner, check the sharing rules, account teams, and account territory.

Access Type	Description
Sharing rules	The user received access because he or she has been included in a relevant sharing rule. If the sharing rule uses public groups (or other categories such as roles) to grant access, check your public groups to see if the user has been included in the group.
Manual shares	The user received access through the Sharing button of the record. Only the record owner, an administrator, or a user above the owner in the role hierarchy can create or remove a manual share on the record.
Account Teams and Territory	The user has been added to an Account Team by the account owner, an administrator, a user above the owner in the role hierarchy, or an account team member. If your organization uses territory management, check if the user who has access is higher in the territory hierarchy than the account owner. Managers gain the same access as their subordinates. Additionally, if the user is a member of Group A, which is a member of Group B, he or she gets access to all accounts shared to Group B, at the same level of access as members of Group B.

SEE ALSO:

[Control Who Sees What](#)

[Financial Services Cloud Administrator Guide: Who Has Access to Account Records with Compliant Data Sharing?](#)

[Resolving Insufficient Privileges Errors](#)

Considerations for Making Sharing Updates

Review these considerations before making sharing changes, such as updates to organization-wide defaults, sharing rules, account ownerships, or group memberships.

General

- When you make certain updates to sharing settings or related features, such as groups, users, territories, or roles, group membership or sharing rule recalculation occurs to ensure that record access is evaluated correctly. Depending on the nature of the updates and configuration of your org, these sharing calculations can take a while to complete.
- Configuration changes that cause sharing rule recalculation include:
 - Changing an organization's default sharing model
 - Creating, editing, or deleting sharing rules
 - Creating or transferring any records
 - Updating public group members
 - Creating or activating a user
 - Changing users' roles or updating the role hierarchy
 - Adding or removing users from territories
 - Reparenting territories
 - Making changes to roles, territories, or public groups involved in sharing rules
- Configuration changes that cause group membership recalculation include:
 - Changing or reparenting roles
 - Adding or removing users from territories
 - Updating public group members

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, and Developer** Editions

- Updating portal account ownership if the new owner has a different role
- Configuration changes that don't cause group membership or sharing rule recalculation include:
 - Territory realignment
 - Updates to sharing sets

Optimization

- Contact Salesforce Customer Support to enable the defer sharing calculations feature. You can defer sharing calculations if you must make large-scale or high-impact changes that trigger sharing recalculation, and want to suspend some automatic sharing calculations to a later time to prevent timeouts or performance issues. For more information, see [Defer Sharing Calculations](#).
- Check to see if any user owns more than 10,000 records of an object, which can cause performance issues. We recommend that you distribute records among a larger group of records before making sharing updates. For more information, see [Ownership Data Skew](#) in the Designing Record Access for Enterprise Scale guide.
- If not yet enabled in your org, enable faster account sharing recalculation. For more information, see the [Faster Account Sharing Recalculation](#) knowledge article.

Deferring Sharing Calculations

- Deferring sharing calculations is intended for operations like large-scale maintenance updates or org realignments that require group membership or sharing rule recalculation.
- Even if you're making only a few configuration changes, consider deferring sharing calculations if the number of affected records or users is very large. For example, you make changes to only a few sharing rules, but for objects that have a significant volume of data. Or, you must edit a few owner-based sharing rules, but this change impacts a large number of users who own the records being shared.
- Changes that aren't directly related to updating your sharing settings can also impact sharing recalculation and benefit from deferring sharing calculations. For example, you upload a large volume of data for one or more objects that have many existing sharing rules.
- If you defer sharing rule calculations, only updates that involve sharing rules, whether directly or indirectly, are deferred, while other sharing-related changes are still processed immediately. To give a few examples, if you create sharing rules or update roles that are referenced in sharing rules, the resulting recalculations are paused. However, if you create manual shares, update teams or queues, or update roles that aren't referenced in any sharing rules, those changes are still evaluated immediately.
- If you defer group membership calculations, membership changes involving individual users are still reflected immediately. However, membership changes related to nested groups or due to role hierarchy changes aren't reflected until after group membership calculations are resumed and you complete a full recalculation. Any change in record access resulting from membership changes also isn't processed until calculation is resumed and you complete a full recalculation.
- If you find that organizational changes and sharing rule updates typically complete quickly enough to be scheduled into the workday or periods of lower activity, you're unlikely to benefit substantially from deferring sharing calculations.
- If you defer sharing calculations, you must always complete a full sharing rule recalculation after you resume group membership or sharing rule calculations. This recalculation ensures that all of your changes are reflected in your sharing rules. If you don't do a full sharing rule recalculation, there can be issues with record access behavior.
- We recommend that you resume sharing calculations immediately after making your changes. Then, start the full sharing rule recalculation as soon as possible during a period of low activity. By resuming sharing immediately, new updates are processed immediately, meaning there are fewer changes that must be recalculated. Completing the full sharing recalculation in a timely manner then ensures that record access behaves as expected without significant lag time.

Testing

- Test making your updates, including resuming sharing recalculation if applicable, in a full copy sandbox before you make these changes in production. This test allows you to both identify any potential issues that can take time and get an estimate of how long the whole process will take in production.
- The full copy sandbox should mimic your current product environment as closely as possible. We recommend using a sandbox refreshed within the last 30 days. In addition, all major changes must be reflected in the sandbox.

Timing

- Plan for a maintenance window that's sufficiently long to complete your changes and for the sharing recalculation to complete.
- Schedule the maintenance window for a period of low activity in your org, such as a weekend.

Organization-Wide Sharing Defaults

Define the default access level for an object's records with organization-wide sharing settings. Organization-wide sharing settings can be set separately for custom objects and many standard objects. You can set different levels of access for internal, external, and guest users.

Watch how you can restrict access to records owned by other users.

 [Watch a video](#)

For most objects, organization-wide sharing settings can be set to Private, Public Read Only, or Public Read/Write. In environments where the organization-wide sharing setting for an object is Private or Public Read Only, an admin can grant users additional access to records by setting up a role hierarchy or defining sharing rules. However, sharing rules can only be used to grant additional access—they can't be used to restrict access to records beyond what was originally specified with the organization-wide sharing defaults.

For information on designing your sharing setup to improve performance and speed up sharing changes, see the [Designing Record Access for Enterprise Scale](#) guide.

SEE ALSO:

- [Set Your Internal Organization-Wide Sharing Defaults](#)
- [Organization-Wide Default Access Settings](#)
- [Default Organization-Wide Access Levels](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions.

Set Your Internal Organization-Wide Sharing Defaults

Internal organization-wide sharing defaults set the baseline access for your internal users for your records. You can set the defaults separately for different objects.

Watch how you can restrict access to records owned by other users.

 [Watch a video](#)

1. From Setup, in the **Quick Find** box, enter *Sharing Settings*, then select **Sharing Settings**.
2. Click **Edit** in the Organization-Wide Defaults area.
3. For each object, select the default internal access that you want to use. For information on setting the default external access, see [External Organization-Wide Defaults Overview](#).
4. To disable automatic access using your hierarchies for custom objects, deselect **Grant Access Using Hierarchies**. You can only deselect this setting for custom objects that don't have a default access of Controlled by Parent. For more information, see [Controlling Access Using Hierarchies in Salesforce Help](#).

When you update organization-wide defaults, sharing recalculation applies the access changes to your records. If you have a lot of data, the update can take longer.

If you're increasing the default access, such as from Public Read Only to Public Read/Write, your changes take effect immediately. All users get access based on the updated default access. Sharing recalculation is then run asynchronously to ensure that all redundant access from manual or sharing rules is removed. When the default access for contacts is Controlled by Parent and you increase the default access for accounts, opportunities, or cases, the changes take effect after recalculation is run. If you're decreasing the default access, such as from Public Read/Write to Public Read Only, your changes take effect after recalculation is run.

You'll receive a notification email when the recalculation completes. Refresh the Sharing Settings page to see your changes. You can also monitor the progress of your organization-wide default updates on the Background Jobs page or view recent sharing operations on the View Setup Audit Trail page.

The organization-wide sharing default setting can't be changed for some objects:

- Service contracts are always Private.
- User provisioning requests are always Private.
- The ability to view or edit a document, report, or dashboard is based on a user's access to the folder in which it's stored.
- Users can view forecasts only of users and territories below them in the forecast hierarchy, unless forecast sharing is enabled.
- When a custom object is on the detail side of a master-detail relationship with a standard object, its organization-wide default is set to Controlled by Parent and it is not editable.
- The organization-wide default settings can't be changed from private to public for a custom object if Apex code uses the sharing entries associated with that object. For example, if Apex code retrieves the users and groups who have sharing access on a custom object `Invoice__c` (represented as `Invoice__share` in the code), you can't change the object's organization-wide sharing setting from private to public.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To set default sharing access:

- [Manage Sharing](#)

 **Note:** Also, if the default access for Account is set to Private, the default access for Opportunity and Case must be set to Private as well. The default access for Contact must be set to Private or Controlled by Parent.

SEE ALSO:

[Organization-Wide Default Access Settings](#)

[Organization-Wide Sharing Defaults](#)

[Designing Record Access for Enterprise Scale](#)

External Organization-Wide Defaults Overview

External organization-wide defaults provide separate organization-wide defaults for internal and external users. They simplify your sharing rules configuration and improve recalculation performance. Additionally, you can easily see which information is being shared to external users.

For example, to configure more restrictive access for external users, set the default internal access to Public Read Only or Public Read/Write and the default external access to Private. These settings also speed up performance for reports, list views, searches, and API queries.

 **Note:** The external access level for an object can't be more permissive than the internal access level.

You can set external organization-wide defaults for these objects. Your org might have other objects whose external organization-wide defaults can be modified.

- Account
- Asset
- Case
- Campaign
- Contact
- Individual
- Lead
- Opportunity
- Order
- User
- Custom Objects

External organization-wide defaults aren't available for some objects, but you can achieve the same behavior with sharing rules. Set the default access to Private and create a sharing rule to share records with all internal users.

External users include:

- Authenticated website users
- Chatter external users
- Site users
- Customer Portal users
- High-volume Experience Cloud site users
- Partner Portal users
- Service Cloud Portal users

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

 **Note:** Chatter external users have access to only the User object.

Guest users aren't considered external users. Guest users' org-wide defaults are set to Private for all objects, and this access level can't be changed.

Learn more about external org-wide default settings in this video.

 [Watch a video](#)

SEE ALSO:

[Organization-Wide Sharing Defaults](#)

[Set Your External Organization-Wide Sharing Defaults](#)

[Organization-Wide Default Access Settings](#)

[Designing Record Access for Enterprise Scale](#)

Set Your External Organization-Wide Sharing Defaults

External organization-wide defaults enable you to set a different default access level for external users.

 **[other]:** Where possible, we changed noninclusive terms to align with our company value of Equality. We maintained certain terms to avoid any effect on customer implementations.

Before you set the external organization-wide defaults, make sure that they're enabled. From Setup, in the Quick Find box, enter *Sharing Settings*, then select **Sharing Settings**, and click the **Enable External Sharing Model** button. External organization-wide defaults are automatically enabled in all orgs created in Spring '20 or after and in all orgs where Salesforce Experiences or portals are enabled.

 **Important:** After it's enabled, the External Sharing Model can't be disabled. You can still manually set **Default External Access** and **Default Internal Access** to the same access level for each object.

When you first enable external organization-wide defaults, the default internal access and default external access are set to the original default access level. For example, if your organization-wide default for contacts is Private, the default internal access and default external access are Private as well. To secure access to your objects, we recommend that you set your external organization-wide defaults to Private.

 **Note:** Keep in mind these access level exceptions:

- After you enable external organization-wide defaults, the external access levels for User and newly created custom objects are set to Private by default.
- In orgs created after Spring '20, the default external access level is set to Private for all objects.
- Objects whose external org-wide defaults can't be set to private can't be viewed by external users in reports.

To set the external organization-wide default for an object:

1. From Setup, in the Quick Find box, enter *Sharing Settings*, then select **Sharing Settings**.
2. Click **Edit** in the Organization-Wide Defaults area.
3. For each object, select the default access you want to use.

You can assign the following access levels.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To set default sharing access:

- [Manage Sharing](#)

Access Level	Description
Controlled by Parent	Users can perform actions (such as view, edit, delete) on a record on the detail side of a master-detail relationship if they can perform the same action on all associated master records. For contacts, <code>Controlled by Parent</code> must be set for both the default internal and external access.
Private	Only users who are granted access by ownership, permissions, role hierarchy, manual sharing, or sharing rules can access the records.
Public Read Only	All users can view all records for the object.
Public Read/Write	All users can view and edit all records for the object.

 **Note:** The default external access level must be more restrictive or equal to the default internal access level. For example, you can have a custom object with default external access set to Private and default internal access set to Public Read Only.

4. Click **Save**.

You can monitor the progress of your organization-wide default updates on the Background Jobs page or view recent sharing operations on the View Setup Audit Trail page.

SEE ALSO:

[External Organization-Wide Defaults Overview](#)

Default Organization-Wide Access Levels

Review the default organization-wide access levels for each object.

In Salesforce orgs created before Spring '20, when you first enable external organization-wide defaults, the default internal access and default external access are set to the original default access level. The only exceptions are User and newly created custom objects, which are set to Private by default.

In orgs created after Spring '20, the default external access level is set to Private for all objects, unless the default internal access level is Controlled by Parent.

Object	Default Internal Access	Default External Access (in orgs created before Spring '20)	Default External Access (in orgs created after Spring '20)
Account	Public Read/Write	Public Read/Write	Private
Activity	Private	Private	Private
Asset	Controlled by Parent	Controlled by Parent	Controlled by Parent
Calendar	Hide Details and Add Events	Hide Details and Add Events	Hide Details and Add Events
Campaign	Public Full Access	Public Full Access	Private

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions.

Object	Default Internal Access	Default External Access (in orgs created before Spring '20)	Default External Access (in orgs created after Spring '20)
Case	Public Read/Write/Transfer	Public Read/Write/Transfer	Private
Contact	Controlled by Parent	Controlled by Parent	Controlled by Parent
Contract	Public Read/Write	Public Read/Write	Private
Custom Object	Public Read/Write	Public Read/Write (created before enabling external org-wide defaults) or Private (created after enabling external org-wide defaults)	Private
Flow Interview	Private	Private	Private
Lead	Public Read/Write/Transfer	Public Read/Write/Transfer	Private
Opportunity	Public Read Only	Public Read Only	Private
Price Book	Use	Use	Use
Service Contract	Private	Private	Private
User	Public Read Only	Private	Private

SEE ALSO:

[Organization-Wide Sharing Defaults](#)

[Set Your Internal Organization-Wide Sharing Defaults](#)

Organization-Wide Default Access Settings

For most objects, you can assign default access to Controlled by Parent, Private, Public Read Only, or Public Read/Write. Other access levels, like Public Full Access and View Only, are available for only specific objects.

These access levels apply to custom objects and most standard objects.

Field	Description
Controlled by Parent	<p>A user can perform an action (such as view, edit, or delete) on a contact or order based on whether he or she can perform that same action on the record associated with it.</p> <p>For example, if a contact is associated with the Acme account, then a user can only edit that contact if he or she can also edit the Acme account.</p>
Private	<p>Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records.</p> <p>For example, if Tom is the owner of an account, and he's assigned to the role of Western Sales, reporting to Carol (who is in the role of VP of Western Region Sales), then Carol can also view, edit, and report on Tom's accounts.</p>
Public Read Only	<p>All users can view and report on records but not edit them. Only the owner, and users above that role in the hierarchy, can edit those records.</p> <p>For example, Sara is the owner of ABC Corp. Sara is also in the role Western Sales, reporting to Carol, who is in the role of VP of Western Region Sales. Sara and Carol have full read/write access to ABC Corp. Tom (another Western Sales Rep) can also view and report on ABC Corp, but can't edit it.</p>
Public Read/Write	<p>All users can view, edit, and report on all records.</p> <p>For example, if Tom is the owner of Trident Inc., all other users can view, edit, and report on the Trident account. However, only Tom can alter the sharing settings or delete the Trident account.</p>

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

Only Custom Objects are available in **Database.com**

USER PERMISSIONS

To set default sharing access:

- Manage Sharing

Field	Description
Public Read/Write/Transfer	All users can view, edit, transfer, and report on all records. Only available for cases or leads. For example, if Alice is the owner of ACME case number 100, all other users can view, edit, transfer ownership, and report on that case. But only Alice can delete or change the sharing on case 100.
Public Full Access	All users can view, edit, transfer, delete, and report on all records. Only available for campaigns. For example, if Ben is the owner of a campaign, all other users can view, edit, transfer, or delete that campaign.

 **Note:** To use cases effectively, set the organization-wide default for Account, Contact, Contract, and Asset to Public Read/Write.

Personal Calendar Access Levels

Field	Description
Hide Details	Others can see whether the user is available at given times, but can't see any other information about the nature of events in the user's calendar.
Hide Details and Add Events	In addition to the sharing levels set by Hide Details, users can insert events in other users' calendars.
Show Details	Users can see detailed information about events in other users' calendars.
Show Details and Add Events	In addition to the sharing levels set by Show Details, users can insert events in other users' calendars.
Full Access	Users can see detailed information about events in other users' calendars, insert events in other users' calendars, and edit existing events in other users' calendars.

 **Note:** Regardless of the organization-wide defaults that have been set for calendars, all users can invite all other users to events.

Price Book Access Levels

Field	Description
Use	All users can view price books and add them to opportunities. Users can add any product within that price book to an opportunity.
View Only	All users can view and report on price books but only users with the "Edit" permission on opportunities or users that have been

Field	Description
	manually granted use access to the price book can add them to opportunities.
No Access	Users can't see price books or add them to opportunities. Use this access level in your organization-wide default if you want only selected users to access selected price books. Then, manually share the appropriate price books with the appropriate users.

Activity Access Levels

Field	Description
Private	Only the activity owner, and users above the activity owner in the role hierarchy, can edit and delete the activity; users with read access to the record to which the activity is associated can view and report on the activity.
Controlled by Parent	A user can perform an action (such as view, edit, transfer, and delete) on an activity based on whether he or she can perform that same action on the records associated with the activity. For example, if a task is associated with the Acme account and the John Smith contact, then a user can only edit that task if he or she can also edit the Acme account and the John Smith record.

User Access Levels

Field	Description
Private	All users have read access to their own user record and those below them in the role hierarchy.
Public Read Only	All users have read access on one another. You can see all users' detail pages. You can also see all users in lookups, list views, ownership changes, user operations, and search.

SEE ALSO:

[Set Your Internal Organization-Wide Sharing Defaults](#)

Controlling Access Using Hierarchies

Determine whether users have access to records they don't own, including records to which they don't have sharing access, but someone below them in the hierarchy does.

 **[other]:** Where possible, we changed noninclusive terms to align with our company value of Equality. We maintained certain terms to avoid any effect on customer implementations.

Watch how you can use the role hierarchy to extend access to records.

 [Watch a video](#)

Beyond setting the organization-wide sharing defaults for each object, you can specify whether users have access to the data owned by or shared with their subordinates in the hierarchy. For example, the role hierarchy automatically grants record access to users above the record owner in the hierarchy. By default, the `Grant Access Using Hierarchies` option is enabled for most standard objects, and it can only be changed for custom objects.

To control sharing access using hierarchies for any custom object, from Setup, in the Quick Find box, enter *Sharing Settings*, then select **Sharing Settings**. Next, click **Edit** in the Organization Wide Defaults section. The `Grant Access Using Hierarchies` is enabled for most standard objects, but not all of them. You can modify this option for custom objects by deselecting it.

Implementation Notes

- Regardless of your organization's sharing settings, users can gain access to records they don't own through other means such as user permissions like "View All Data," sharing rules, or manual sharing of individual records.
- If the `Grant Access Using Hierarchies` option is deselected, users that are higher in the role or territory hierarchy don't receive automatic access. But some, such as those users with the View All and Modify All object permissions and the View All Data and Modify All Data system permissions can still access records that they don't own.
- If you disable the `Grant Access Using Hierarchies` option, sharing with a role or territory and subordinates only shares with the users directly associated with the role or territory selected. Users in roles or territories above them in the hierarchies don't gain access.
- If your organization disables the `Grant Access Using Hierarchies` option, activities that are associated with a custom object are still visible to users above the activity's assignee in the role hierarchy.
- If a master-detail relationship is broken by deleting the relationship, the former detail custom object's default setting is automatically reverted to Public Read/Write and `Grant Access Using Hierarchies` is selected by default.
- The `Grant Access Using Hierarchies` option affects which users gain access to data when something is shared with public groups, personal groups, queues, roles, or territories. For example, the **View All Users** option displays group members and people above them in the hierarchies when a record is shared with them using a sharing rule or manual sharing and the `Grant Access Using Hierarchies` option is selected. When the `Grant Access Using Hierarchies` option isn't selected, some users in these groups no longer have access. This list covers the access reasons that depend on the `Grant Access Using Hierarchies` option.

These reasons always gain access:

- Group Member
- Queue Member
- Role Member
- Member of Subordinate Role

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

Territories aren't available in **Database.com**

USER PERMISSIONS

To set default sharing access and change the `Grant Access Using Hierarchies` option:

- [Manage Sharing](#)

Territory Member

Member of Subordinate Territory

These reasons only gain access when using hierarchies:

Manager of Group Member

Manager of Queue Member

Manager of Role

Manager of Territory

User Role Manager of Territory

- When you deselect `Grant Access Using Hierarchies`, always notify users of the changes in report results that they can expect due to losing visibility of their subordinates' data. For example, selecting `My team's...` in the View dropdown list returns records owned by the user. It doesn't include records owned by their subordinates. To be included in this type of report view, records from subordinates must be explicitly shared with that user by some other means such as a sharing rule or a manual share. So if no records are shared with you manually, the `My...` and `My team's...` options in the View dropdown list return the same results. But choosing the `Activities with...` any custom object report type when creating a custom report returns activities assigned to you as well as your subordinates in the role hierarchy.
- Record access granted to users via sharing sets isn't extended to their superiors in the role hierarchy.

SEE ALSO:

[Create a User Role](#)

Create a User Role

Salesforce offers a user role hierarchy that you can use with sharing settings to determine the levels of access that users have to your Salesforce org's data. Roles within the hierarchy affect access on key components such as records and reports.

For information on designing your sharing setup to improve performance and speed up sharing changes, see the [Designing Record Access for Enterprise Scale](#) guide.

Users at any role level can view, edit, and report on all data that's owned by or shared with users below them in their role hierarchy. If your org's sharing model specifies different sharing access for an object, then sharing defers to the OWD settings. Specifically, in the Organization-Wide defaults related list, you can disable the **Grant Access Using Hierarchies** option for a custom object. When disabled, only the record owner and users who are granted access by the organization-wide defaults receive access to the object's records.

1. From Setup, in the Quick Find box, enter `Roles`, then select **Roles**.
2. If the "Understanding Roles" page is displayed, click **Set Up Roles**.
3. Find the role under which you want to add the new role. Click **Add Role**.
4. Add a Label for the role. The Role Name field autopopulates.
5. Specify who the role reports to. The field is already populated with the role name under which you added the new role, but you can also edit the value here.
6. Optionally, specify how the role name is displayed in reports. If the role name is long, consider using an abbreviation for reports.
7. Specify the role's access to contacts, opportunities, and cases.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To view roles and role hierarchy:

- View Roles and Role Hierarchy

To create, edit, and delete roles:

- Manage Roles

To assign users to roles:

- Manage Internal Users

For example, you can set the contact access so that users in a role can edit all contacts associated with accounts that they own. This access applies regardless of who owns the contacts. And you can set the opportunity access so that users in a role can edit all opportunities associated with accounts that they own. This access also applies regardless of who owns the opportunities.

8. Click **Save.**

Portal user roles aren't included on the role hierarchy setup page.

When you edit groups, roles, and territories, sharing rules are recalculated to add or remove access as needed.

Depending on the nature of your updates and your org's setup, these sharing calculations can take a while to complete. If you experience sharing evaluations or timeouts, consider deferring sharing calculations before making large-scale updates, and then restart and recalculate sharing at a later time. For more information, see [Defer Sharing Calculations](#) in Salesforce Help.



Note: After you share a folder with a role, it's visible only to users in that role, not to superior roles in the hierarchy.

Assign Users to Roles

Quickly assign users to a particular role.

1. From Setup, in the Quick Find box, enter *Roles*, then select **Roles**.
2. Click **Assign** next to the name of the desired role.



Note: You can also access this page by clicking **Assign Users to Role** on the role's detail page. Large organizations should consider assigning roles via the [SOAP API](#) for efficiency.

3. Make a selection from the dropdown list to show the available users.
4. Select a user on the left, and click **Add** to assign the user to this role.
5. Click **Save**.



Note: Removing a user from the Selected Users list deletes the role assignment for that user.

SEE ALSO:

[Create a User Role](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To assign users to roles:

- [Manage Internal Users](#)

View and Edit Roles

From the Role Detail page, you can view and edit information about the role and its assigned users.

 **Note:** When you edit groups, roles, and territories, sharing rules are recalculated to add or remove access as needed.

1. From Setup, in the Quick Find box, enter *Roles*, and then select **Roles**.
2. Click the role's name.
3. In the Role Detail related list:
 - To view the role detail page for a parent or sibling role, click the role name in the Hierarchy or Siblings list.
 - To edit the role details, click **Edit**.
 - To remove the role from the hierarchy, click **Delete**.
 - To view sharing group members, click **Role** or **Role and Subordinates** in the Sharing Groups field.
4. In the Users in Role related list:
 - To [assign a user to the role](#), click **Assign Users to Role**.
 - To [add a user](#) to your organization, click **New User**.
 - To [modify user information](#), click **Edit** next to a user name.
 - To view a user's details, click the user's full name, alias, or username. When Active is selected, the user can log into Salesforce. [Deactivated users](#), such as employees who are no longer with your company, can't log in to Salesforce.
 - To show a filtered list of items, select a predefined list from the *view* dropdown list, or click **Create New View** to define your own custom views. To edit or delete any view you created, select it from the *view* dropdown list and click **Edit**.

SEE ALSO:

[Sharing Considerations](#)

Guidelines for Success with Roles

Understand key rule behaviors, and apply best practices for success with roles.



For best practices on designing record access in a large organization, see [Designing Record Access for Enterprise Scale](#).

- To simplify user management in Salesforce orgs with large numbers of users, enable delegated administrators to manage users in specified roles and all subordinate roles.
- In Salesforce orgs created in Spring '21 or later, you can create up to 5,000 roles. In orgs created before Spring '21, you can create up to 500 roles and can contact Salesforce Customer Support to increase this limit.
- Every user must be assigned to a role, or their data won't display in opportunity reports, forecast roll-ups, and other displays based on roles.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To view role details:

- View Roles and Role Hierarchy

To edit and delete roles:

- Manage Roles

To view users:

- View Setup and Configuration

To edit users:

- Manage Internal Users

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

- Put all users that require visibility to the entire org at the highest level in the hierarchy.
- Don't create individual roles for each title at your company. Instead, define a hierarchy of roles to control access of information entered by users in lower-level roles.
- Create roles only for your current requirements. Don't create temporary placeholder roles in anticipation of future needs.
- Don't use reporting requirements to determine what hierarchy levels you need.
- When you change a user's role, the sharing rules for the new role are applied.
- Salesforce Knowledge users can modify category visibility settings on the role detail page.
- When an account owner isn't assigned a role, the sharing access for related contacts is Read/Write, provided the organization-wide default for contacts isn't Controlled by Parent. Sharing access on related opportunities and cases is No Access.
- If your organization uses Territory Management, forecasts are based on the territory hierarchy rather than the role hierarchy.
- To prevent disruptions, avoid changing the role hierarchy during business hours.

Performance

- To avoid performance issues, we recommend that no single user owns more than 10,000 records of an object. For users who must own more than that number of objects, don't assign them a role or place them in a separate role at the top of the hierarchy. It's also important to keep that user out of public groups potentially used as the source for sharing rules.
- To improve performance, minimize the number of levels in your role hierarchy. Eliminate roles that aren't needed, and delete sharing rules that grant access to records already shared via the role hierarchy.

Role Fields

The fields that comprise a role entry have specific purposes. Refer to this table for descriptions of each field and how it functions in a role.

The visibility of fields depends on your organization's permissions and sharing settings.

Field	Description
Case Access	Specifies whether users can access other users' cases that are associated with accounts the users own. This field isn't visible if your organization's sharing model for cases is Public Read/Write.
Contact Access	Specifies whether users can access other users' contacts that are associated with accounts the users own. This field isn't visible if your organization's sharing model for contacts is Public Read/Write or Controlled by Parent.
Label	The name used to refer to the role or title of position in any user interface pages, for example, Western Sales VP.
Modified By	The name of the user who last modified this role's details, and the date and time that the role was modified.
Opportunity Access	Specifies whether users can access other users' opportunities that are associated with accounts

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To create or edit roles:

- Manage Roles

Field	Description
Partner Role	<p>the users own. This field isn't visible if your organization's sharing model for opportunities is Public Read/Write.</p> <p>Indicates whether this role is associated with a partner account. This field is available only when a customer or partner site or portal is enabled for the organization.</p> <p>If this checkbox is selected, you can't edit the role. The default number of roles in site and portal accounts is three. You can reduce the number of roles or add roles to a maximum of three.</p>
Role Name	The unique name used by the API and managed packages.
Role Name as displayed on reports	A role name that appears in reports. When editing a role, if the Role Name is long, you can enter an abbreviated name in this field.
Sharing Groups	<p>These groups are automatically created and maintained. The Role group contains all users in this role plus all users in roles above this role. The Role and Subordinates group contains all users in this role plus all users in roles above and below this role in the hierarchy. The Role and Internal Subordinates group (available if Salesforce Experiences or portals are enabled for your organization) contains all users in this role. It also contains all users in roles above and below this role, excluding site and portal users.</p>
This role reports to	The role above this role in the hierarchy.

SEE ALSO:

[Create a User Role](#)

Role and Territory Sharing Groups

Salesforce creates sharing groups for each role and territory in your Salesforce org.

For each [role](#) in your hierarchy, Salesforce automatically creates sharing groups, which you can use in sharing rules and manual sharing:

- Role—users in the role plus users in roles above it in the hierarchy.
- Role and Subordinates—users in the role plus users in roles above and below it in the hierarchy.
- Role and Internal Subordinates—users in the role, plus users in roles above and below it in the hierarchy, excluding portal or site users. This group is only available when Salesforce Experiences or portals are enabled for your organization.
- Roles, Internal and Portal Subordinates—users in the role, plus users in roles above and below it in the hierarchy, including portal or site users. This group is only available when Salesforce Experiences or portals are enabled for your organization.

If Enterprise Territory Management is enabled for your org, each territory has sharing groups:

- Territory—users in the territory plus users in territories above it in the hierarchy.
- Territory and Subordinates—users in the territory plus users in territories above and below it in the hierarchy.

Managers in the Role Hierarchy

The Managers in the Role Hierarchy related list shows all of the users above you in the hierarchy. These users have the same access to your data as you do—they have access to all data you own or that has been shared with you.

1. From your personal settings, in the Quick Find box, enter *Advanced User Details*, then select **Advanced User Details**. No results? In the Quick Find box, enter *Personal Information*, then select **Personal Information**.
2. Scroll down to see the Managers in the Role Hierarchy related list.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

Enterprise Territory Management is available in: **Developer** and **Performance** Editions and in **Enterprise** and **Unlimited** Editions with the Sales Cloud

USER PERMISSIONS

To view users:

- View Setup and Configuration

To edit users:

- Manage Internal Users

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

Sharing Rules

Use sharing rules to extend sharing access to users in public groups, roles, or territories. Sharing rules give particular users greater access by making automatic exceptions to your org-wide sharing settings.

Watch how you can grant access to records using sharing rules.

 [Watch a video](#)

Like role hierarchies, a sharing rule can never be stricter than your org-wide default settings. It simply allows greater access for particular users.

You can base a sharing rule on record ownership or other criteria. After you select which records to share, you define which groups or users to extend access to and what level of access they have.

 **Note:** You can define up to 300 total sharing rules for each object, including up to 50 criteria-based or guest user sharing rules, if available for the object.

You can create these types of sharing rules. Your org could have other objects that are available for sharing rules.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer Editions**

See [Sharing Rule Considerations](#) for more information on availability.

Type	Based On	Set Default Sharing Access For
Account sharing rules	Account owner or other criteria, including account record types or field values	Accounts and their associated contracts, opportunities, cases, and optionally, contacts and orders
Asset sharing rules	Asset owner or other criteria, including asset record types or field values	Individual assets
Campaign sharing rules	Campaign owner or other criteria, including campaign record types or field values	Individual campaigns
Case sharing rules	Case owner or other criteria, including case record types or field values	Individual cases and associated accounts
Contact sharing rules	Contact owner or other criteria, including contact record types or field values	Individual contacts and associated accounts
Custom object sharing rules	Custom object owner or other criteria, including custom object record types or field values	Individual custom object records
Data privacy sharing rules	Data privacy record owner or other criteria, including field values. Data privacy records are based on the Individual object.	Individual data privacy records
Knowledge article sharing rules	Knowledge article owner or other criteria, including Knowledge object record types or field values	Individual article versions
Flow interview sharing rules	Flow interview owner or other criteria, such as the pause reason	Individual flow interviews
Lead sharing rules	Lead owner or other criteria, including lead record types or field values	Individual leads

Type	Based On	Set Default Sharing Access For
Location sharing rules	Location owner or other criteria	Individual locations
Maintenance plan sharing rules	Maintenance plan owner or other criteria	Individual maintenance plans
Opportunity sharing rules	Opportunity owner or other criteria, including opportunity record types or field values	Individual opportunities and their associated accounts
Order sharing rules	Order owner or other criteria, including order record types or field values	Individual orders
Product item sharing rules	Product item owner or other criteria	Individual product items
Product request sharing rules	Product request owner only; criteria-based sharing rules aren't available	Individual product requests
Product transfer sharing rules	Product transfer owner only; criteria-based sharing rules aren't available	Individual product transfers
Return order sharing rules	Return order owner or other criteria	Individual return orders
Service appointment sharing rules	Service appointment owner or other criteria	Individual service appointments
Service contract sharing rules	Service contract owner or other criteria	Individual service contracts
Service crew sharing rules	Service crew owner only; criteria-based sharing rules aren't available	Individual service crews
Service resource sharing rules	Service resource owner or other criteria	Individual service resources
Service territory sharing rules	Service territory owner or other criteria	Individual service territories
Shipment sharing rules	Shipment owner only; criteria-based sharing rules aren't available	Individual shipments
Time sheet sharing rules	Time sheet owner only; criteria-based sharing rules aren't available	Individual time sheets
User sharing rules	Group membership or other criteria, including username and whether the user is active	Individual users
User provisioning request sharing rules	User provisioning request owner, only; criteria-based sharing rules aren't available	Individual user provisioning requests
Work order sharing rules	Work order owner or other criteria, including work order record types or field values	Individual work orders
Work type sharing rules	Work type owner or other criteria	Individual work types

 **Note:** Developers can use Apex to programmatically share custom objects based on record owners but not other criteria.

SEE ALSO:

[Sharing Rule Considerations](#)

Sharing Rule Types

You can base a sharing rule on record ownership or other criteria.

Owner-Based Sharing Rules

An owner-based sharing rule opens access to records owned by certain users. For example, a company's sales managers need to see opportunities owned by sales managers in a different region. The U.S. sales manager could give the APAC sales manager access to the opportunities owned by the U.S. team using owner-based sharing.

Criteria-Based Sharing Rules

A criteria-based sharing rule determines with whom to share records based on field values. For example, you have a custom object for job applications, with a custom picklist field named "Department." A criteria-based sharing rule could share all job applications in which the Department field is set to "IT" with all IT managers in your organization.

 **Note:**

- A criteria-based sharing rule is based on record values and not the record owners. However, a role or territory hierarchy still allows users higher in the hierarchy to access the records.
- You can't use Apex to create a criteria-based sharing rule. And you can't test criteria-based sharing using Apex.
- Starting with API version 24.0, you can use the Metadata API SharingRules type to create criteria-based sharing rules.

You can create criteria-based sharing rules for accounts, assets, campaigns, cases, contacts, leads, opportunities, work orders, and custom objects. For the sharing criteria, record types and these field types are supported.

- Auto Number
- Checkbox
- Date
- Date/Time
- Email
- Lookup Relationship (to user ID or queue ID)
- Number
- Percent
- Phone
- Picklist
- Text
- Text Area

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

See [Sharing Rule Considerations](#) for more information on availability.

- URL

 **Note:** Text and Text Area are case-sensitive. For example, a criteria-based sharing rule that specifies “Manager” in a text field doesn’t share records that have “manager” in the field. To create a rule with several common cases of a word, enter each value separated by a comma.

Guest User Sharing Rules

A guest user sharing rule is a special type of criteria-based sharing rule and the only way to grant record access to unauthenticated guest users.

 **Warning:** The guest user sharing rule type grants access to guest users without login credentials. By creating a guest user sharing rule, you're allowing immediate and unlimited access to all records matching the sharing rule's criteria to anyone. To secure your Salesforce data and give your guest users access to what they need, consider all the use cases and implications of creating this type of sharing rule. Implement security controls that you think are appropriate for the sensitivity of your data. Salesforce is not responsible for any exposure of your data to unauthenticated users based on this change from default settings.

You can also create sharing rules based on group membership.

SEE ALSO:

[Sharing Rules](#)

Create Sharing Rules

You can create sharing rules based on the record owner or other criteria, and sharing rules that grant record access to unauthenticated guest users. You can also create sharing rules based on group membership for the User object.

You can define up to 300 total sharing rules for each object, including up to 50 criteria-based or guest user sharing rules, if available for the object.

For information on designing your sharing setup to improve performance and speed up sharing changes, see the [Designing Record Access for Enterprise Scale](#) guide.

SEE ALSO:

[Create Owner-Based Sharing Rules](#)

[Create Criteria-Based Sharing Rules](#)

[Create Guest User Sharing Rules](#)

[Create Sharing Rules Based on Group Membership](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Create Owner-Based Sharing Rules

An owner-based sharing rule opens access to records owned by certain users.

For information on designing your sharing setup to improve performance and speed up sharing changes, see the [Designing Record Access for Enterprise Scale](#) guide.

1. If you plan to include public groups in your sharing rule, confirm that the appropriate groups have been created.
2. From Setup, in the Quick Find box, enter *Sharing Settings*, then select **Sharing Settings**.
3. In the Sharing Rules related list for the object, click **New**.
4. Enter the label name and rule name. The label name appears on the user interface. The rule name is a unique name used by the API and managed packages.
5. Optionally, enter a description of the sharing rule, up to 1,000 characters.
6. For the rule type, select **Based on record owner**.
7. Specify which users' records are shared. For owned by members of, select a category from the first dropdown list and a set of users from the second dropdown list or lookup field.
8. Specify the users who get access to the data. For Share with, select a category from the first dropdown list and a set of users from the second dropdown list or lookup field.
9. Select sharing access settings for users. Some access settings aren't available for some objects or in some situations.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To create sharing rules:

- **Manage Sharing**

Access Setting	Description
Private	Users can't view or update records, unless access is granted outside of this sharing rule. Available only for associated contacts, opportunities, and cases.
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.
Full Access	Users in the selected group, role, or territory can view, edit, transfer, delete, and share the record, just like the record's owner. With a Full Access sharing rule, users can also view, edit, delete, and close activities associated with the record if the org-wide sharing setting for activities is Controlled by Parent. Available for campaigns only.

 **Note:** `Contact Access` isn't available when the organization-wide default for contacts is set to Controlled by Parent.

10. Click **Save**.

After updates to sharing rules, sharing rules are recalculated to add or remove access as needed. Depending on the nature of your updates and your org's setup, these sharing calculations can take awhile to complete. If you experience sharing evaluations or timeouts, consider deferring sharing calculations before making large-scale updates, and then restart and recalculate sharing at a later time. For more information, see [Defer Sharing Calculations](#) in Salesforce Help.

Create Criteria-Based Sharing Rules

A criteria-based sharing rule determines who to share records with based on field values.

For information on designing your sharing setup to improve performance and speed up sharing changes, see the [Designing Record Access for Enterprise Scale](#) guide.

1. To include public groups in your sharing rule, confirm that those groups were created.
2. From Setup, in the Quick Find box, enter *Sharing Settings*, and then select **Sharing Settings**.
3. In the Sharing Rules related list for the object, click **New**.
4. Enter the label name and rule name. The label name appears on the user interface. The rule name is a unique name used by the API and managed packages.
5. Optionally, enter a description of the sharing rule of up to 1,000 characters.
6. For the rule type, select **Based on criteria**.
7. Specify the field, operator, and value criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value is always a literal number or string. To change the AND relationship between filters, click **Add Filter Logic**. The value criteria is limited to 240 characters, and strings or picklist values that go beyond this limit are truncated.

 **Note:** You can use a field that's not supported by criteria-based sharing rules. Create a workflow rule or Apex trigger to copy the value of the field into a text or numeric field. Then use that field as the criterion.

8. If available, select whether to include records owned by users who can't have an assigned role, such as high-volume users and system users. This setting is enabled by default and can't be edited after you save the rule.

 **Note:** To include these users in criteria-based sharing rules that were created before Spring '22, delete the rule and select **Include records owned by users who can't have an assigned role** when you recreate it.

9. Specify the users who get access to the data. For Share with, select a category from the first dropdown list and a set of users from the second dropdown list or lookup field.
10. Select sharing access settings for users. Some access settings aren't available for some objects or in some situations.

Access Setting	Description
Private	Users can't view or update records, unless access is granted outside of this sharing rule. Available only for associated contacts, opportunities, and cases.
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.
Full Access	Users in the selected group, role, or territory can view, edit, transfer, delete, and share the record, just like the record's owner. With a Full Access sharing rule, users can also view, edit, delete, and close activities associated with the record if the org-wide sharing setting for activities is Controlled by Parent. Available for campaigns only.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer Editions**

USER PERMISSIONS

To create sharing rules:

- Manage Sharing

 **Note:** `Contact Access` isn't available when the organization-wide default for contacts is set to Controlled by Parent.

11. Save your work.

After updates to sharing rules, sharing rules are recalculated to add or remove access as needed. Depending on the nature of your updates and your org's setup, these sharing calculations can take awhile to complete. If you experience sharing evaluations or timeouts, consider deferring sharing calculations before making large-scale updates, and then restart and recalculate sharing at a later time. For more information, see [Defer Sharing Calculations](#) in Salesforce Help.

Create Guest User Sharing Rules

A guest user sharing rule is a special type of criteria-based sharing rule and the only way to grant record access to unauthenticated guest users. Guest user sharing rules can only grant Read Only access.

 **Important:** You must create guest user sharing rules to open up record access to guest users. Keep in mind that the guest user sharing rule type grants access to users without login credentials. By creating a guest user sharing rule, you're allowing immediate and unlimited access to all records matching the sharing rule's criteria to anyone. To secure your Salesforce data and give your guest users access to what they need, consider all the use cases and implications of creating this type of sharing rule. Implement security controls that you think are appropriate for the sensitivity of your data. Salesforce is not responsible for any exposure of your data to unauthenticated users based on this change from default settings.

1. From Setup, in the Quick Find box, enter *Sharing Settings*, then select **Sharing Settings**.
2. In the Sharing Rules related list for the object, click **New**.
3. Enter the label name and rule name. The label name appears on the user interface. The rule name is a unique name used by the API and managed packages.
4. Optionally, enter a description of the sharing rule, up to 1,000 characters.
5. For the rule type, select **Guest user, based on criteria**.
6. Specify the field, operator, and value criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value is always a literal number or string. To change the AND relationship between filters, click **Add Filter Logic**. The value criteria is limited to 240 characters, and strings or picklist values that go beyond this limit are truncated.

 **Note:** To use a field that's not supported by criteria-based sharing rules, create a workflow rule or Apex trigger to copy the value of the field into a text or numeric field. Then use that field as the criterion.

7. If available in your org, select whether to include records owned by high-volume community or site users. By default, sharing rules include only records owned by authenticated users, guest users, and queues.

 **Tip:** High-volume users don't have roles and include the External Apps, Customer Community, High Volume Customer Portal, and Authenticated Website license types. For more information, see [About High-Volume Community or Site Users](#) in Salesforce Help.

8. Specify the users who get access to the data.

9. Click **Save**.

SEE ALSO:

[About High-Volume Community or Site Users](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To create sharing rules:

- [Manage Sharing](#)

Create Sharing Rules Based on Group Membership

For the User object, you can create sharing rules based on group membership.

1. If you plan to include public groups in your sharing rule, confirm that the appropriate groups have been created.
2. From Setup, in the Quick Find box, enter *Sharing Settings*, then select **Sharing Settings**.
3. In the Sharing Rules related list for the User object, click **New**.
4. Enter the label name and rule name. The label name appears on the user interface. The rule name is a unique name used by the API and managed packages.
5. Optionally, enter a description of the sharing rule, up to 1,000 characters.
6. For the rule type, select **Based on group membership**.
7. Select which users to be shared. For Users are a member of, select a category from the first dropdown list and a set of users from the second dropdown list or lookup field.
8. Specify the users who get access to the data. For Share with, select a category from the first dropdown list and a set of users from the second dropdown list or lookup field.
9. Select sharing access settings for users.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

10. Click **Save**.

Sharing Rule Categories

When you define a sharing rule, you can choose from the following categories in the `owned by members of` and `Share with` dropdown lists. Depending on the type of sharing rule and the features enabled for your organization, some categories may not appear.

 **Note:** You can't include high-volume Experience Cloud site users in sharing rules because they don't have roles and can't be in public groups.

Category	Description
Managers Groups	All direct and indirect managers of a user.
Manager Subordinates Groups	A manager and all direct and indirect reports who he or she manages.
Queues	All records owned by the queue, excluding records owned by individual members of the queue. Available only in the <code>owned by members of</code> list.
Public Groups	All public groups defined by your administrator. If Salesforce Experiences or portals are enabled for your organization, the All Partner Users or All Customer Portal Users group displays.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To create sharing rules:

- Manage Sharing

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

See [Sharing Rule Considerations](#) for more information on availability.

Category	Description
	These groups include all partner or customer users, respectively, allowed to access your site or portal, except for high-volume users.
Roles	All roles defined for your organization, excluding site and portal roles. This includes all of the users in the specified role.
Portal Roles	All roles defined for your organization's site or portal. This includes all users in the specified role, except high-volume users. A site or portal role name includes the name of the account that it's associated with, except for person accounts, which include the user Alias .
Roles and Subordinates	All roles defined for your organization. This includes all of the users in the specified role plus all of the users in roles below that role. This is only available when no Salesforce Experience sites or portals are enabled for your organization.
Portal Roles and Subordinates	All roles defined for your organization's site or portal. This includes all of the users in the specified role plus all of the users below that role in the site or portal role hierarchy, except for high-volume users. A site or portal role name includes the name of the account that it's associated with, except for person accounts, which include the user Alias .
Roles and Internal Subordinates	All roles defined for your organization. This includes all of the users in the specified role plus all of the users in roles below that role, excluding site and portal roles. This category is displayed only if Salesforce Experiences or portals are enabled for your organization.
Roles, Internal and Portal Subordinates	All roles defined for your organization. This includes all of the users in the specified role plus all of the users in roles below that role, including site and portal roles.
Territories	All territories defined for your organization.
Territories and Subordinates	All territories defined for your organization. This includes the specified territory plus all territories below it.
Guest User	All unauthenticated users in a site.

SEE ALSO:

[Sharing Rules](#)[Sharing Records with Manager Groups](#)

Edit Sharing Rules

For a sharing rule based on owner or group membership, you can edit only the sharing access settings. For a sharing rule based on other criteria, you can edit the criteria and sharing access settings.

1. From Setup, in the Quick Find box, enter *Sharing Settings*, then select **Sharing Settings**.
2. In the Sharing Rules related list for the object, click **Edit**.
3. Change the label and rule name if desired.
4. If you selected a rule that's based on owner or group membership, skip to the next step. If you selected a criteria-based or guest user sharing rule, specify the criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value must be a literal number or string. To change the AND relationship between filters, click **Add Filter Logic**.

 **Note:** You must create guest user sharing rules to open up record access to guest users. Keep in mind that the guest user sharing rule type grants access to users without login credentials. By creating a guest user sharing rule, you're allowing immediate and unlimited access to all records matching the sharing rule's criteria to anyone. To secure your Salesforce data and give your guest users access to what they need, consider all the use cases and implications of creating this type of sharing rule. Implement security controls that you think are appropriate for the sensitivity of your data. Salesforce is not responsible for any exposure of your data to unauthenticated users based on this change from default settings.

5. Select sharing access settings for users. Some access settings aren't available for some objects or in some situations.

Access Setting	Description
Private	Users can't view or update records, unless access is granted outside of this sharing rule. Available only for associated contacts, opportunities, and cases.
Read Only	Users can view, but not update, records. Guest user sharing rules can only grant Read Only access.
Read/Write	Users can view and update records.
Full Access	Users in the selected group, role, or territory can view, edit, transfer, delete, and share the record, just like the record's owner. With a Full Access sharing rule, users can also view, edit, delete, and close activities associated with the record if the org-wide sharing setting for activities is Controlled by Parent. Available for campaigns only.

 **Note:** `Contact Access` isn't available when the organization-wide default for contacts is set to Controlled by Parent.

6. Click **Save**.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

See [Sharing Rule Considerations](#) for more information on availability.

USER PERMISSIONS

To create sharing rules:

- [Manage Sharing](#)

After updates to sharing rules, sharing rules are recalculated to add or remove access as needed. Depending on the nature of your updates and your org's setup, these sharing calculations can take awhile to complete. If you experience sharing evaluations or timeouts, consider deferring sharing calculations before making large-scale updates, and then restart and recalculate sharing at a later time. For more information, see [Defer Sharing Calculations](#) in Salesforce Help.

SEE ALSO:

[Sharing Rules](#)

Sharing Rule Considerations

Review these considerations before using sharing rules.

- General Considerations
 - You can use sharing rules to grant wider access to data. You can't restrict access below your organization-wide default levels.
 - To create sharing rules, your organization-wide defaults must be Public Read Only or Private.
 - If multiple sharing rules give a user different levels of access to a record, the user gets the most permissive access level.
 - Sharing rules automatically grant additional access to related records. For example, opportunity sharing rules give role or group members access to the account associated with the shared opportunity. Contact and case sharing rules also provide the role or group members with access to the associated account.
 - Users in the role hierarchy are automatically granted the same access that users below them in the hierarchy have from a sharing rule provided that the object is a standard object or the Grant Access Using Hierarchies option is selected.
 - Users who don't have licenses that support roles can only be included in some types of sharing rules, to receive access and to have records that they own shared. High-volume community or site users, Chatter External, and Chatter Free users can't be included in owner-based sharing rules. You can share records owned by high-volume users in guest user or criteria-based sharing rules.
 - Users who can't have an assigned role can be included in criteria-based sharing rules that were created after the Spring '22 release. To include these users in criteria-based sharing rules that were created before Spring '22, delete the rule and select **Include records owned by users who can't have an assigned role** when you recreate it. These users can't be included in other types of sharing rules.
 - In criteria-based sharing rules, you can't use lookup fields, encrypted fields, formula fields, or fields whose values are derived from other fields on the record.
- Availability
 - Account, campaign, case, contact, lead, opportunity, and custom object sharing rules are available for Enterprise, Performance, Unlimited, and Developer Editions.
 - Only account, asset, campaign, and contact sharing rules are available in Professional Edition.
 - Only custom object sharing rules are available in Database.com
 - Criteria-based sharing rules aren't available for all objects.
 - Your org can have other objects that are available for sharing rules. To see which sharing rules are available, see the Sharing Settings setup page.
- Updating
 - Creating an owner-based sharing rule with the same source and target groups as an existing rule overwrites the existing rule.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer Editions**

- After a sharing rule is saved, you can't change the `Share with` field settings when you edit the sharing rule.
 - Sharing rules apply to all new and existing records that meet the definition of the source dataset.
 - Sharing rules apply to active and inactive users.
 - When you change the access levels for a sharing rule, all records are automatically updated to reflect the new access levels.
 - When you delete a sharing rule, the sharing access created by that rule is removed.
 - When you modify which users are in a group, role, or territory, the sharing rules are reevaluated to add or remove access as necessary.
 - When you transfer records from one user to another, the sharing rules are reevaluated to add or remove access to the transferred records as necessary.
 - Changing sharing rules can require changing a large number of records at once. If your request is queued to process these changes efficiently, you receive an email notification when the process has completed.
 - Lead sharing rules don't automatically grant access to lead information after leads are converted into account, contact, and opportunity records.
- Site and Portal Users
 - You can create rules to share records between most types of site or portal and Salesforce users. And you can create sharing rules between site or portal users from different accounts as long as their license type supports roles. But you can't include high-volume community or site users in owner-based sharing rules because they don't have roles and can't be in public groups. You can share records owned by high-volume users in guest user or criteria-based sharing rules.
 - After enabling digital experiences, existing sharing rules automatically extend access to external users. This change occurs because sharing rules that grant access to Roles and Subordinates are converted to grant access to Roles, Internal and Portal Subordinates instead. To ensure that external users can't access records or folders containing sensitive data, update your sharing rules.
 - You can easily convert sharing rules that include Roles, Internal, and Portal Subordinates to include Roles and Internal Subordinates instead by using the Convert External User Access Wizard on the Digital Experiences Settings Setup page. You can use this wizard to convert any publicly accessible report, dashboard, and document folders to folders that are accessible by all users except for external users. For more information, see [Considerations for the Convert External User Access Wizard](#).
 - You can only use guest user sharing rules to share records with unauthenticated guest users.
 - For more information on using sharing rules in Experience Cloud sites, check out this video.
 [Watch a video](#)
 - Managed Package Fields If a criteria-based sharing rule references a field from a licensed managed package whose license has expired, (`expired`) is appended to the label of the field. The field label appears in the field dropdown list on the rule's definition page in Setup. Criteria-based sharing rules that reference expired fields aren't recalculated, and new records aren't shared based on those rules. But the sharing of existing records before the package's expiration is preserved.

SEE ALSO:

[Sharing Rules](#)[Considerations for the Convert External User Access Wizard](#)[Sharing Rules for Communities](#)

Defer Sharing Calculations

Performing a large number of configuration changes can lead to very long sharing rule evaluations or timeouts. To avoid these issues, an administrator can suspend sharing calculations, specifically for sharing rules and group membership, then resume calculations during an organization's maintenance period.

 **Note:** The defer sharing calculation feature isn't enabled by default. To enable it for your organization, contact Salesforce Customer Support.

By default, sharing rules and group membership are recalculated after certain updates to related features, such as sharing settings, roles, territories, groups, and users.

Type of Sharing Calculation	Occurs When You
Sharing Rule	<ul style="list-style-type: none"> • Change an organization's default sharing model • Create, edit, or delete sharing rules • Create or transfer any records • Update public group members • Create or activate a user • Change users' roles or update the role hierarchy • Add or remove users from territories • Reparent territories • Make changes to roles, territories, or public groups involved in sharing rules
Group Membership	<ul style="list-style-type: none"> • Change or reparent roles • Add or remove users from territories • Update public group members • Update portal account ownership if the new owner has a different role

When you defer sharing calculations, most sharing evaluations are disabled and access configuration changes don't take effect until you resume sharing and recalculate sharing rules. You can defer sharing calculations if you make a large number of changes that trigger sharing recalculation, and want to suspend the automatic sharing calculations to a later time to prevent timeouts or performance issues.

Keep in mind that sharing updates aren't evaluated while sharing calculations are deferred. You must also remember to restart sharing calculations and complete a full recalculation to avoid record access inconsistencies. To ensure that your changes are successful and the impact to your users is minimal, review [Considerations for Making Sharing Updates](#) before deferring group membership or sharing rule calculations.

SEE ALSO:

[Recalculate Sharing Rules Manually](#)

[Designing Record Access for Enterprise Scale](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

Defer Sharing Rule Calculations

If you're making a large number of changes that affect sharing rules, including changes to sharing rules, roles, territories, or public groups, you can temporarily suspend automatic sharing rule calculations and resume them after you finish your updates. You must resume calculations and do a full sharing rule recalculation, or you can experience sharing inconsistencies in your records.

When you make any of these changes, sharing rules are automatically recalculated to add or remove access as necessary:

- Change an organization's default sharing model
- Create, edit, or delete sharing rules
- Create or transfer any records
- Update public group members
- Create or activate a user
- Change users' roles or update the role hierarchy
- Add or remove users from territories
- Reparent territories
- Make changes to roles, territories, or public groups involved in sharing rules

If any of these changes affect large groups of users or related features, your updates can cause performance issues or sharing rule calculation timeouts. You can temporarily defer sharing rule calculations before you make your changes. After you finish your updates, you must resume sharing rule calculations and do a full sharing recalculation. Review [Considerations for Making Sharing Updates](#) before deferring sharing rule calculations.

We recommend that you resume sharing calculations immediately after making your changes, and then start the full sharing rule recalculation as soon as possible during a period of low activity. By resuming sharing calculations immediately, new updates are processed immediately, meaning there are fewer changes that must be recalculated. Completing the full sharing recalculation in a timely manner then ensures that record access behaves as expected without significant lag time.

 **Note:** The defer sharing calculation feature isn't enabled by default. To enable it for your organization, contact Salesforce Customer Support.

1. From Setup, in the Quick Find box, enter *Defer Sharing Calculations*, and then select **Defer Sharing Calculations**.
2. In the Sharing Rule Calculations related list, click **Suspend**.
3. Make changes to sharing rules, roles, territories, or public groups participating in sharing rules.
4. To enable sharing rule calculations again, click **Resume**.
5. To manually recalculate sharing rules, click **Recalculate**.

 **Important:** After you resume sharing rule calculations, you must click Recalculate to do a full sharing rule recalculation. Otherwise, changes that you made while calculations were suspended aren't reflected in your sharing rules.

When sharing is recalculated, Salesforce also runs all Apex sharing recalculations.

SEE ALSO:

[Defer Group Membership Calculations](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer Editions**

See [Sharing Rule Considerations](#) for more information on availability.

USER PERMISSIONS

To defer (suspend and resume) and recalculate sharing rules:

- Manage Users
- AND
- Manage Sharing Calculation Deferral

Defer Group Membership Calculations

If you're making changes to groups or related features that affect many records, you can temporarily suspend automatic group membership calculations and resume them after you finish your updates. You must resume calculations and do a full sharing rule recalculation, or you can experience sharing inconsistencies in your records.

When you make changes to roles, territories, groups, or users, or change ownership of portal accounts, group membership is automatically recalculated to add or remove access as necessary. Changes can include adding or removing a user from a group or changing a role to allow access to different sets of reports.

If you're making large-scale changes that can cause performance issues or group membership calculation timeouts, you can temporarily defer group membership calculations before you make your changes. After you make your changes, you must resume group membership calculations and do a full sharing recalculation. Review [Considerations for Making Sharing Updates](#) before deferring group membership calculations.

We recommend that you resume sharing calculations immediately after making your changes, and then start the full sharing rule recalculation as soon as possible during a period of low activity. By resuming sharing immediately, new updates are processed immediately, meaning there are fewer changes that must be recalculated. Completing the full sharing recalculation in a timely manner then ensures that record access behaves as expected without significant lag time.

 **Note:** The defer sharing calculation feature isn't enabled by default. To enable it for your organization, contact Salesforce Customer Support.

1. From Setup, in the Quick Find box, enter *Defer Sharing Calculations*, and then select **Defer Sharing Calculations**.
2. In the Group Membership Calculations related list, click **Suspend**.

 **Note:** Suspending group membership calculations also suspends sharing rule calculations.

3. Make your changes to roles, territories, groups, users, or portal account ownership.
4. To enable group membership calculations again, click **Resume**. Group membership and sharing rule recalculation begins automatically.
5. To recalculate sharing rules, select **Yes** when asked if you want to automatically recalculate sharing rules. Or, in the Sharing Rule Calculations related list, click **Recalculate**.

 **Important:** After you resume group membership calculations, you must do a full sharing rule recalculation. Otherwise, changes that you made while calculations were suspended aren't reflected in your sharing rules.

SEE ALSO:

[Defer Sharing Calculations](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To defer (suspend and resume) sharing calculations:

- Manage Users

AND

Manage Sharing Calculation Deferral

Recalculate Sharing Rules Manually

When you make changes to sharing settings, groups, roles, and territories, sharing rules are reevaluated to add or remove access as necessary. You can manually recalculate sharing rules if sharing rule updates have failed or aren't working as expected.

Sharing rule recalculation occurs automatically after adding or removing individual users from a group, role, or territory, changing which role a particular role reports to, changing which territory a particular territory is subordinate to, or adding or removing a group from within another group.

You can also recalculate sharing rules manually using the Recalculate buttons on the Sharing Rules related lists. Manually recalculate sharing rules only if updates have failed or record access isn't working as expected. Because recalculating sharing rules can take a while, you only want to initiate a manual recalculation in case of errors.

 **Note:** If enabled in your org, you can temporarily defer sharing rule calculations. This feature is useful for large-scale maintenance operations or org realignments planned during low activity periods in your org. After this work is completed, you must resume sharing rule calculations and manually initiate a full sharing rule recalculation to prevent errors. For more information, see [Defer Sharing Calculations](#).

To manually recalculate an object's sharing rules:

1. From Setup, in the Quick Find box, enter *Sharing Settings*, and then select **Sharing Settings**.
2. In the Sharing Rules related list for the object you want, click **Recalculate**.
3. If you want to monitor the progress of a recalculation, from Setup, in the Quick Find box, enter *Background Jobs*, and then select **Background Jobs**.

You receive an email notification when the recalculation is completed for all affected objects.

 **Note:** The **Recalculate** button is disabled when group membership or sharing rule calculations are deferred.

SEE ALSO:

[Sharing Rules](#)

[Defer Sharing Calculations](#)

[Monitor Background Jobs](#)

[Designing Record Access for Enterprise Scale](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer Editions**

See [Sharing Rule Considerations](#) for more information on availability.

USER PERMISSIONS

To recalculate sharing rules:

- [Manage Sharing](#)

Automatic Recalculation of Org-Wide Defaults and Sharing Rules

When you update organization-wide defaults or sharing rules, automatic sharing recalculation is processed asynchronously and in parallel.

Review these considerations for automatic sharing recalculation behavior.

General

- If sharing rules are recalculated for accounts, cases, contacts, or opportunities, sharing rules are also recalculated for the other three objects. This behavior occurs because cases, contacts, and opportunities are child objects of accounts.
- To maintain implicit sharing between accounts and child records, updating the org-wide default on an account or its child objects disables further org-wide default and sharing rule updates on them. For example, when you update an opportunity sharing rule and recalculation is in progress, you can't update the org-wide default or sharing rules for accounts, contacts, opportunities, and cases.
- In the Background Jobs page, these processes correspond to these job subtypes: **Account — Extra Parent Access Removal** and **Account — Parent Access Grant**. Additionally, deleting a sharing rule corresponds to the job subtype **Object — Access Cleanup**, denoting that irrelevant share rows are removed.
- When sharing is recalculated, Salesforce also runs all Apex sharing recalculations.

Monitoring

- You receive an email notification upon completion of the recalculation.
- You can monitor the progress of your parallel sharing rule or organization-wide default recalculation on the Background Jobs page or view recent sharing operations on the View Setup Audit Trail page.

Share Locks

- You can't modify the org-wide defaults when a sharing rule recalculation for any object is in progress. Similarly, you can't modify sharing rules when recalculation for an org-wide default update is in progress.
- You can make changes to the org-wide defaults and sharing rules for other objects.

SEE ALSO:

[Monitor Background Jobs](#)

[Recalculate Sharing Rules Manually](#)

[Built-in Sharing Behavior](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer Editions**

See [Sharing Rule Considerations](#) for more information on availability.

Asynchronous Deletion of Obsolete Shares

Obsolete shares are removed asynchronously after groups are deleted or users are deactivated so that admins can perform other operations without waiting for shares to be deleted.

Many sharing operations have an immediate impact on the visibility of records within the system. For example, deleting a group revokes the access granted to that group via sharing rules or manual shares. When deleting a group, the shares to the group become obsolete. Obsolete shares are deleted asynchronously during off-peak hours to minimize wait time during this operation.

Members of these groups lose access to records immediately. Users higher than these members in the role hierarchy also lose access to the records.

- Public groups
- Queues
- Roles
- Territories

When deactivating a user, the user's manually assigned shares and their team shares are deleted asynchronously. Until the obsolete shares are deleted, users higher in the role hierarchy retain access to the records associated with these shares. If that visibility is a concern, remove the record access granted to the user before deactivating the account. All other user-related share types are deleted immediately when the user is deactivated.

Manual Sharing

Manual sharing gives other users access to certain types of records, including accounts, contacts, and leads.

Sometimes, granting access to one record includes access to all its associated records. For example, if you grant another user access to an account, the user automatically has access to all the opportunities and cases associated with that account.

To grant access to a record, you must be one of the following users.

- The record owner
- A user in a role above the owner in the hierarchy (if your organization's sharing settings control access through hierarchies)
- A user with the Modify All permission for the object
- A system administrator

 **Note:** If you're manually sharing an opportunity, contact, or case, the users you share it with must have at least Read access to the associated parent account via sharing features or you must have the ability to also share the account. You have the ability to share the account if you are the account owner, are a system administrator, are above the account owner in the role hierarchy, and/or have the Modify All permission on accounts. If you have the ability to share the account itself, the users you share the opportunity, contact, or case with are automatically given Read access to the parent account.

If a user transfers ownership of a record, Salesforce deletes any manual shares created by the original record owner, which can cause users to lose access. When account ownership is transferred, manual shares created by the original account owner on child records, such as opportunities and cases, are also deleted.

When the parent account for a contact associated with a portal or community user changes, manual shares for custom object records that were shared with the portal or community user are deleted.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer Editions**

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer Editions**

 **Note:** When the parent account for an opportunity changes, manual shares for the opportunity are deleted if the user making the change isn't allowed to share the new parent account. But when the new parent account owner, someone above them in the role hierarchy, or a Salesforce admin changes the parent account, the manual shares aren't deleted.

When an opportunity is closed and the owner of the opportunity's parent account changes, manual shares for the opportunity are deleted even when opportunity splits are enabled.

[Grant Access to Records with Manual Sharing in Lightning Experience](#)

Give specific users access to certain types of records with manual sharing.

[Grant Access to Records with Manual Sharing in Salesforce Classic](#)

Use manual sharing to give specific other users access to certain types of records, including accounts, contacts, and leads.

[Manual Sharing Considerations](#)

When you grant access to records with manual sharing, there are some considerations to keep in mind.

Grant Access to Records with Manual Sharing in Lightning Experience

Give specific users access to certain types of records with manual sharing.

1. Click **Sharing** on the record that you want to share.
2. In the Search box, enter the groups, users, roles, or territories to add.

Use the search dropdown to filter for a group type. Depending on the data in your org, your options can include:

Type	Description
Managers Groups	All direct and indirect managers of a user.
Manager Subordinates Groups	Managers and all the direct and indirect reports that they manage.
Public Groups	All public groups defined by your administrator.
Users	All users in your org. Doesn't include portal users.
Roles	All roles defined for your org, including all users in each role.
Roles and Subordinates	All users in the role plus all users in roles below that role in the hierarchy. Only available when no portals are enabled for your org. After enabling Salesforce Experiences, manual shares accessible to Roles and Subordinates are automatically converted to be shared with Roles, Internal, and Portal Subordinates. To secure external users' access, remove Roles, Internal, and Portal Subordinates from the Share With list of your manual shares. Add Roles and Internal Subordinates instead.

EDITIONS

Available in: Lightning Experience ([not available in all orgs](#))

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Type	Description
Roles and Internal Subordinates	All roles defined for your org. Includes all users in the specified role and all users in roles below that role. Doesn't include partner portal and Customer Portal roles.
Roles and Internal and Portal Subordinates	Adds a role and its subordinate roles. Includes all users in that role plus all users in roles below that role. Only available when a partner or Customer Portal is enabled for your org. Includes portal roles and users.
Territories	For orgs that use territory management, all territories defined for your org, including all users in each territory. Only the territories in the active territory model are available.
Territories and Subordinates	For orgs that use territory management, all users in the territory plus the users below that territory. Only the territories in the active territory model are available.

- Choose the access level for the record that you're sharing and any associated records that you own.

Access Level	Description
Full Access	User can view, edit, delete, and transfer the record. User can also extend sharing access to other users. But the user can't grant Full Access to other users.
Read/Write	User can view and edit the record, and add associated records, notes, and attachments to it.
Read Only	User can view the record, and add associated records to it. They can't edit the record or add notes or attachments.
Private	User can't access the record in any way.

 **Note:**

- If you're sharing an opportunity, contact, or case, the users you share it with must have at least Read access to the associated parent account via sharing features or you must have the ability to also share the account. You have the ability to share the account if you are the account owner, are a system administrator, are above the account owner in the role hierarchy, and or have the Modify All permission on accounts. If you have the ability to share the account itself, the users you share the opportunity, contact, or case with are automatically given Read access to the parent account.
- `Contact Access` isn't available when the org-wide default for contacts is set to Controlled by Parent.

- Save your changes.

On the Sharing page, you can click **Edit** for a summary of the groups of users that this record is shared with. For full details on who has access to the record, click **View Sharing Hierarchy**.

Grant Access to Records with Manual Sharing in Salesforce Classic

Use manual sharing to give specific other users access to certain types of records, including accounts, contacts, and leads.

1. Click **Sharing** on the record you want to share.
2. Click **Add**.
3. From the **Search** dropdown list, select the type of group, user, role, or territory to add. Depending on the data in your org, your options can include:

Type	Description
Managers Groups	All direct and indirect managers of a user.
Manager Subordinates Groups	Managers and all the direct and indirect reports they manage.
Public Groups	All public groups defined by your administrator.
Personal Groups	All personal groups defined by the record owner. Only record owners can share with their personal groups.
Users	All users in your org. Doesn't include portal users.
Roles	All roles defined for your org, including all users in each role.
Roles and Subordinates	<p>All users in the role plus all users in roles below that role in the hierarchy. Only available when no portals are enabled for your org.</p> <p>After enabling Salesforce Experiences, manual shares accessible to Roles and Subordinates are automatically converted to be shared with Roles, Internal, and Portal Subordinates. To secure external users' access, remove Roles, Internal and Portal Subordinates from the Share With list of your manual shares, and add Roles and Internal Subordinates instead.</p>
Roles and Internal Subordinates	All roles defined for your org, including all users in the specified role, all the users in roles below that role. However, it doesn't include partner portal and Customer Portal roles.
Roles and Internal and Portal Subordinates	Adds a role and its subordinate roles. Includes all users in that role plus all users in roles below that role. Only available when a partner or Customer Portal is enabled for your org. Includes portal roles and users.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

Type	Description
Territories	For organizations that use territory management, all territories defined for your org, including all users in each territory. Only the territories in the active territory model are available.
Territories and Subordinates	For orgs that use territory management, all users in the territory plus the users below that territory. Only the territories in the active territory model are available.

 **Note:** With more than 2,000 users, roles, and groups, if your query doesn't match any items in a particular category, that category doesn't show up in the Search dropdown menu. For example, if none of your group names contain the string CEO, after searching for CEO, the Groups option no longer appears in the dropdown. If you enter a new search term, all categories are still searched even if they don't appear in the list. You can repopulate the dropdown by clearing your search terms and pressing **Find**.

- Choose the specific groups, users, roles, or territories whom you want to give access by adding their names to the Share With list. Use the **Add** and **Remove** arrows to move the items from the Available list to the Share With list.

 **Note:** You can't grant access to unauthenticated guest users with manual sharing.

- Choose the access level for the record you're sharing and any associated records that you own.

Access Level	Description
Full Access	User can view, edit, delete, and transfer the record. User can also extend sharing access to other users. But the user can't grant Full Access to other users.
Read/Write	User can view and edit the record, and add associated records, notes, and attachments to it.
Read Only	User can view the record, and add associated records to it. They can't edit the record or add notes or attachments.
Private	User can't access the record in any way.

 **Note:**

- If you're sharing an opportunity, contact, or case, the users you share it with must have at least Read access to the associated parent account via sharing features or you must have the ability to also share the account. You have the ability to share the account if you are the account owner, are a system administrator, are above the account owner in the role hierarchy, and or have the Modify All permission on accounts. If you have the ability to share the account itself, the users you share the opportunity, contact, or case with are automatically given Read access to the parent account.
- `Contact Access` isn't available when the org-wide default for contacts is set to Controlled by Parent.

- Select the reason you're sharing the record so users and administrators can understand.
- Save your changes.

Manual Sharing Considerations

When you grant access to records with manual sharing, there are some considerations to keep in mind.

- Experience Cloud sites and the Salesforce mobile app don't support manual sharing in Lightning.
- If you're sharing an opportunity, contact, or case, the users you share it with must have at least Read access to the associated parent account via sharing features or you must have the ability to also share the account. You have the ability to share the account if you are the account owner, are a system administrator, are above the account owner in the role hierarchy, and/or have the Modify All permission on accounts. If you have the ability to share the account itself, the users you share the opportunity, contact, or case with are automatically given Read access to the parent account.
- Apex-managed shares aren't editable.
- Admins can't modify the share access of record owners.
- Personal groups aren't available in Lightning Experience.
- When navigating through a Sharing Hierarchy table, JAWS and NVDA screen readers don't announce that there's a link inside of a table cell, and they don't provide a keyboard shortcut to open the link. Use another form of input or assistive technology instead.
- With more than 2,000 users, roles, and groups, if your query doesn't match any items in a particular category, that category doesn't show up in the Search dropdown menu. For example, if none of your group names contain the string CEO, after searching for CEO, the Groups option no longer appears in the dropdown. If you enter a new search term, all categories are still searched even if they don't appear in the list. You can repopulate the dropdown by clearing your search terms and pressing **Find**.
- You can't grant access to unauthenticated guest users with manual sharing.
- In Lightning Experience, both sharing and the Sharing Hierarchy action are available for custom objects and these standard objects.
 - Account
 - Action Plan
 - Action Plan Template
 - Appointment Invitation
 - Appointment Bundle Configuration
 - Appointment Bundle Policy Service Territories
 - Asset
 - Campaign
 - Case
 - Contact
 - Engagement Interaction
 - Expense
 - Expense Report
 - Flow
 - Job Profile
 - Lead
 - Maintenance Plan
 - Maintenance Work Rule
 - Opportunity
 - Product Item

EDITIONS

Available in: Lightning Experience (not available in all orgs)

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

- Product Request
- Product Service Campaign
- Product Transfer
- Recordset Filter Criteria
- Return Order
- Serialized Product
- Service Appointment
- Service Contract
- Service Crew
- Service Resource
- Service Territory
- Shift
- Shift Pattern
- Survey
- Survey Invitation
- Time Sheet
- Travel Mode
- Video Call
- Warranty Term
- Work Order
- Work Plan
- Work Plan Selection Rule
- Work Plan Template
- Work Step Template
- Work Type
- Work Type Group

Viewing Which Users Have Access to Your Records in Salesforce Classic

When viewing a record, you can view a list of users who have been granted access through sharing. The list includes their access level and an explanation and shows every user who has access that's greater than the org-wide default settings.

 **Note:** Some sharing rules specify access to an object and its associated objects. For sharing rules that specify access for associated object records, the given access level applies to that sharing rule only. For example, if an account sharing rule specifies Private as the access level for associated contacts, a user can access associated contacts via other means. These means include org-wide defaults, the Modify All Data or View All Data permission, or the Modify All or View All permission for contacts.

1. To display a list of users who have access, click **Sharing** on the desired record.
2. To see full details about who has access to this record, click **Expand List**.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

3. To see the reason the user has access to the record, click **Why?** next to a user's name. If there are multiple reasons with different access levels, the user is always granted the most permissive access level. The possible reasons are:

Reason	Description
Account Guest Sharing Rule	The guest user has access via an account guest user sharing rule created by the administrator.
Account Sharing Rule	The user has access via an account sharing rule created by the administrator.
Account Sharing	The user was granted access via the Sharing button on the associated account.
Account Team	The user is a member of the account team.
Account Territory	The account has been assigned to a territory to which the user has access.
Administrator	The user has the "Modify All Data" or "View All Data" administrative permission, or the "Modify All" or "View All" object permission.
Asset Guest Sharing Rule	The guest user has access via an asset guest user sharing rule created by the administrator.
Asset Sharing Rule	The user has access via an asset sharing rule created by the administrator.
Associated Guest User Sharing	The guest user has sharing access to a record associated with the account. To view which associated records the user owns or has been given sharing access to, click the link
Associated Portal User or Role	The portal or site user, or any role above the portal or site user's role, has access to the account for which the portal or site user is a contact.
Associated Record Owner or Sharing	The user owns or has sharing access to a contact or contract associated with the account. To view which associated records the user owns or has been given sharing access to, click the link.
Associated Record Sharing	The user is a member of a share group that has access to a contact or contract that's associated with the account owned by high-volume Experience Cloud site users.
Campaign Guest Sharing Rule	The guest user has access via a campaign guest user sharing rule created by the administrator.
Campaign Sharing Rule	The user has access via a campaign sharing rule created by the administrator.
Case Guest Sharing Rule	The guest user has access via a case guest user sharing rule created by the administrator.
Case Sharing Rule	The user has access via a case sharing rule created by the administrator.

Reason	Description
Contact Guest Sharing Rule	The guest user has access via a contact guest user sharing rule created by the administrator.
Contact Sharing Rule	The user has access via a contact sharing rule created by the administrator.
Group Member	The user has access via a group, such as a Managers Group or Manager Subordinates Group.
Individual Guest Sharing Rule	The guest user has access via an individual guest user sharing rule created by the administrator.
Individual Sharing Rule	The user has access via an individual sharing rule created by the administrator.
Lead Guest Sharing Rule	The guest user has access via a lead guest user sharing rule created by the administrator.
Lead Sharing Rule	The user has access via a lead sharing rule created by the administrator.
Manager of Territory Member	The user has a subordinate in the role hierarchy who is assigned to the territory with which the account is associated.
Manual Sharing	The user has access that was granted via the Sharing button on the record.
Manual Territory Sharing	The account has been manually assigned to a territory to which the user has access.
Opportunity Guest Sharing Rule	The guest user has access via an opportunity guest user sharing rule created by the administrator.
Opportunity Sharing Rule	The user has access via an opportunity sharing rule created by the administrator.
Order Guest Sharing Rule	The guest user has access via an order guest user sharing rule created by the administrator.
Order Sharing Rule	The user has access via an order sharing rule created by the administrator.
Owner	The user owns the record, or the user is a member of the queue that owns the record or above the queue member in the role hierarchy.
Portal Share Group	The user is a member of a share group that has access to records owned by high-volume Experience Cloud site users.
Related Portal User	The portal or site user is a contact on the case.
Role Above Owner or Shared User (Portal Only)	The user's role is above the role of a portal or site user who has access to the record via ownership or sharing.
Sales Team	The user is a member of the opportunity sales team.

Reason	Description
User Sharing Rule	The user has access via a user sharing rule created by the administrator.
User Guest Sharing Rule	The guest user has access via a user guest user sharing rule created by the administrator.
View All Forecasts Permission	The forecasts user has the View All Forecasts permission.

If a user has access to a record as a result of multiple sharing reasons, some reasons are compressed into a single record. That record contains the highest level of permission. The compressed reasons are: Associated Portal User or Role, Associated Record Owner or Sharing, Manual Sharing, and Owner. For example, if a user owns opportunities associated with an account and was also manually given access to that account, the user is listed only one time on sharing pages.

Viewing Which Users Have Access to Your Records in Lightning Experience

When viewing a record, you can view a list of users who have been granted access to the record through sharing. The list includes their access level and an explanation and shows every user who has access that's greater than the org-wide default settings.

Some sharing rules specify access to an object and its associated objects. For sharing rules that specify access for associated object records, the given access level applies to that sharing rule only. For example, if an account sharing rule specifies Private as the access level for associated contacts, a user can access associated contacts via other means. These means include org-wide defaults, the Modify All Data or View All Data permission, or the Modify All or View All permission for contacts.

1. To display a list of users who have access, click **Sharing Hierarchy** from the Action Menu on the desired record.



Note: In editions that support restriction rules, this list can include users who don't have access due to a restriction rule.

2. To see the reason the user has or doesn't have access to the record, click **View** next to a user's name. When you click **View**, all applicable sharing reasons appear. If a restriction rule blocks access to the record, a message is shown to confirm that access is blocked. The possible reasons are.

EDITIONS

Available in: Lightning Experience (not available in all orgs)

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer Editions**

Reason	Description
Account Guest Sharing Rule	The guest user has access via an account guest user sharing rule created by the administrator.
Account Sharing Rule	The user has access via an account sharing rule created by the administrator.
Account Sharing	The user was granted access via the Sharing button on the associated account.
Account Team	The user is a member of the account team.
Account Territory	The account has been assigned to a territory to which the user has access.

Reason	Description
Administrator	The user has the “Modify All Data” or “View All Data” administrative permission, or the “Modify All” or “View All” object permission.
Asset Guest Sharing Rule	The guest user has access via an asset guest user sharing rule created by the administrator.
Asset Sharing Rule	The user has access via an asset sharing rule created by the administrator.
Associated Guest User Sharing	The guest user has sharing access to a record associated with the account. To view which associated records the user owns or has been given sharing access to, click the link.
Associated Portal User or Role	The portal or site user, or any role above the portal or site user's role, has access to the account for which the portal or site user is a contact.
Associated Record Owner or Sharing	The user owns or has sharing access to a contact or contract associated with the account. To view which associated records the user owns or has been given sharing access to, click the link.
Associated Record Sharing	The user is a member of a share group that has access to a contact or contract that's associated with the account owned by high-volume Experience Cloud site users.
Campaign Guest Sharing Rule	The guest user has access via a campaign guest user sharing rule created by the administrator.
Campaign Sharing Rule	The user has access via a campaign sharing rule created by the administrator.
Case Guest Sharing Rule	The guest user has access via a case guest user sharing rule created by the administrator.
Case Sharing Rule	The user has access via a case sharing rule created by the administrator.
Contact Guest Sharing Rule	The guest user has access via a contact guest user sharing rule created by the administrator.
Contact Sharing Rule	The user has access via a contact sharing rule created by the administrator.
Group Member	The user has access via a group, such as a Managers Group or Manager Subordinates Group.
Individual Guest Sharing Rule	The guest user has access via an individual guest user sharing rule created by the administrator.
Individual Sharing Rule	The user has access via an individual sharing rule created by the administrator.
Lead Guest Sharing Rule	The guest user has access via a lead guest user sharing rule created by the administrator.

Reason	Description
Lead Sharing Rule	The user has access via a lead sharing rule created by the administrator.
Manager of Territory Member	The user has a subordinate in the role hierarchy who is assigned to the territory with which the account is associated.
Manual Sharing	The user has access that was granted via the Sharing button on the record.
Manual Territory Sharing	The account has been manually assigned to a territory to which the user has access.
Opportunity Guest Sharing Rule	The guest user has access via an opportunity guest user sharing rule created by the administrator.
Opportunity Sharing Rule	The user has access via an opportunity sharing rule created by the administrator.
Order Guest Sharing Rule	The guest user has access via an order guest user sharing rule created by the administrator.
Order Sharing Rule	The user has access via an order sharing rule created by the administrator.
Owner	The user owns the record, or the user is a member of the queue that owns the record or above the queue member in the role hierarchy.
Portal Share Group	The user is a member of a share group that has access to records owned by high-volume Experience Cloud site users.
Related Portal User	The portal or site user is a contact on the case.
Role Above Owner or Shared User (Portal Only)	The user's role is above the role of a portal or site user who has access to the record via ownership or sharing.
Sales Team	The user is a member of the opportunity sales team.
User Sharing Rule	The user has access via a user sharing rule created by the administrator.
User Guest Sharing Rule	The guest user has access via a user guest user sharing rule created by the administrator.
View All Forecasts Permission	The forecasts user has the View All Forecasts permission.

If multiple sharing reasons give a user access to a record, some sharing reasons can be compressed into a single reason, which shows the most permissive access level, on the Sharing Hierarchy page. These sharing reasons can be compressed.

- Associated Portal User or Role
- Associated Record Owner or Sharing
- Manual Sharing
- Owner

See Account Access from Manual Shares or Account Teams with Reports

See the account records that are shared manually or through account teams in your Salesforce org and which users or groups have access to them. Before building reports, create a custom report type on the Account Share object, which represents sharing entries on an account.

-  **Note:** Currently, you can only report on accounts shared manually or through account teams. The custom report type doesn't include account shares from other features, such as sharing rules, territories, or implicit sharing access.

[Create a Custom Report Type for Account Shares](#)

Before you can build Account Share reports, create a custom report type.

[Report on Who Has Access to Accounts From Manual Shares or Account Teams](#)

Build a report for information on account records shared manually or through account teams in your Salesforce org.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To create and update custom report types:

- Create and Customize Reports
- AND
- Manage Custom Report Types

To create, edit, and delete reports:

- Create and Customize Reports
- AND
- Manage Custom Report Types

To view account share records in reports:

- View All permission on account

Create a Custom Report Type for Account Shares

Before you can build Account Share reports, create a custom report type.

1. From Setup, in the Quick Find box, enter **Report Types**, and then select *Report Types*.
2. Select **Account Share** as the Primary Object.
3. Add a label and description.
4. Choose which category to store the report in.
5. Select a Deployment Status.
6. Click **Next**, and then save.
7. To customize which fields are displayed in the custom report type, in the Fields Available for Reports section, click **Edit Layout**. To add fields, click **Add fields related via lookup**, and then select any of these supported fields: Account Id, Account Name, Group ID, Group Name, Group Type, User Active, User Full Name, User ID, User Type, User Email. Click **OK**, and then click **Save**.
8. Save your work.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To create and update custom report types:

- Create and Customize Reports

AND

Manage Custom Report Types

To view account share records in reports:

- View All permission on account

Report on Who Has Access to Accounts From Manual Shares or Account Teams

Build a report for information on account records shared manually or through account teams in your Salesforce org.

Here's how to configure a sample account share report.

1. Create a new report. Select the custom report type created for account shares.
2. To see all account share records, adjust your filters so that Show Me is set to **All account share** and Created Date is set to **All Time**.
3. Under Columns, select which fields to display.
4. Optionally, to see only account records that are shared manually, add a filter for Row Cause so that the field's value must equal Manual Sharing. Or, to see only account records that are shared through account teams, add a filter for Row Cause so that the field's value must equal Sales Team. There are multiple values available for Row Cause, but only Manual Sharing and Row Cause are supported.
5. Group rows to help with your analysis. For example, group by the account name or ID to see which users have access to each account record. You can also group by the user's name or ID to see which accounts individual users have access to.
6. To help with your analysis, add charts for a visual overview of your data.

 **Note:** For account records shared with users in a specified role, the report displays the role sharing group ID in the Group: Group ID field. The role's ID isn't displayed. For more information, see [Role and Territory Sharing Groups](#) in Salesforce Help.

SEE ALSO:

[Create a Custom Report Type](#)

[Build a Report](#)

Object Reference for the Salesforce Platform: AccountShare

User Sharing

User Sharing enables you to show or hide an internal or external user from another user in your organization.

Watch how you can control the visibility that users have to each other.

 [Watch a video](#)

With User Sharing, you can:

- Assign the "View All Users" permission to users who need to see or interact with all users. This permission is automatically enabled for users who have the "Manage Users" permission.
- Set the [organization-wide default](#) for user records to Private or Public Read Only.
- Create user [sharing rules](#) based on group membership or other criteria.
- Create [manual shares](#) for user records to open up access to individual users or groups.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To create, edit, and delete reports:

- Create and Customize Reports

AND

Manage Custom Report Types

To view account share records in reports:

- View All permission on account

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

- Control the visibility of external users.

SEE ALSO:

[Understanding User Sharing](#)

[Control Which Users Experience Cloud Site Users Can See](#)

Set the Org-Wide Sharing Defaults for User Records

Set the org-wide sharing defaults for the user object before opening up access.

For user records, you can set the organization-wide sharing default to Private or Public Read Only. The default must be set to Private if there is at least one user who shouldn't see a record.

Let's say that your organization has internal users (employees and sales agents) and external users (site or portal users) under different sales agents or accounts, with these requirements:

- Employees can see everyone.
- Sales agents can see employees, other agents, and their own customer user records only.
- External customers can see other customers only if they are under the same agent or account.

To meet these requirements, set the default external access to Private, and extend access using sharing rules, manual sharing, or user permissions.

When the feature is first turned on, the default access setting is Private for external users. The default for internal users is Public Read Only. To change the organization-wide defaults for external access to the user object:

1. From Setup, in the Quick Find box, enter *Sharing Settings*, then select **Sharing Settings**.
2. Click **Edit** in the Organization-Wide Defaults area.
3. Select the default internal and external access you want to use for user records.
The default external access must be more restrictive or equal to the default internal access.
4. Click **Save**.
Users have Read access to those below them in the role hierarchy and full access on their own user record.

SEE ALSO:

[Control Which Users Experience Cloud Site Users Can See](#)
[User Sharing](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To set default sharing access:

- [Manage Sharing](#)

Understanding User Sharing

Review these considerations before you implement user sharing.

Granting access to a user record makes the user's detail page visible to others. It also makes the user visible in lookups, list views, search, and so on.

“View All Users” permission

This permission can be assigned to users who need Read access to all users, regardless of the sharing settings. If you already have the “Manage Users” permission, you're automatically granted the “View All Users” permission.

Organization-wide defaults for user records

This setting defaults to Private for external users and Public Read Only for internal users. When the default access is set to Private, users can only read and edit their own user record. Users with subordinates in the role hierarchy maintain read access to the user records of those subordinates.

User sharing rules

General sharing rule considerations apply to user sharing rules. User sharing rules are based on membership to a public group, role, or territory. Each sharing rule shares members of a source group with those of the target group. You must create the appropriate public groups, roles, or territories before creating your sharing rules. Users inherit the same access as users below them in the role hierarchy.

Manual sharing for user records

Manual sharing can grant read or edit access on an individual user, but only if the access is greater than the default access for the target user. Users inherit the same access as users below them in the role hierarchy. Apex managed sharing isn't supported.

User sharing for external users

Users with the “Manage External Users” permission have access to external user records for Partner Relationship Management, Customer Service, and Customer Self-Service portal users, regardless of sharing rules or organization-wide default settings for User records. The “Manage External Users” permission doesn't grant access to guest or Chatter External users.

High-volume Experience Cloud site users and Chatter users

Only users with roles can be included in sharing rules. For this reason, the user records of high-volume users, Chatter External, and Chatter Free users can't be included in sharing rules, and these users can't be granted access to user records via a sharing rule.

Automated Process and License Manager users

Some special users created for org or app maintenance, such as Automated Process and License Manager users, can't be included in any sharing rules, including user sharing rules.

User sharing compatibility

When the organization-wide default for the user object is set to Private, user sharing doesn't fully support these features.

- Chatter Messenger isn't available for external users. It's available for internal users only when the organization-wide default for the user object is set to Public Read Only.

EDITIONS

Available in: both Salesforce Classic (**not available in all orgs**) and Lightning Experience

Manual sharing available in: Salesforce Classic

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

- Salesforce CRM Content—A user who can create libraries can see users they don't have access to when adding library members.
- Standard Report Types—If the organization-wide default for the user object is Private and the Standard Report Visibility checkbox is selected, a person viewing the report can see the names of users that are listed in the report. To see details such as username and email address, the viewer must have access to the users.

User sharing in Chatter

In Chatter, there are exceptions where users who aren't shared can still see and interact with each other. For example, regardless of user sharing, in a public Chatter group, everyone with access to the group can see all posts. They can also see the names of the users who post and mention users who commented on a post.

For example, you set up user sharing so Mary and Bob can't see or interact with each other. Mary posts on a public Chatter group. She can't mention Bob, because user sharing prevents Bob's name from showing up in the mention dropdown list. However, Bob can see Mary's post and he comments on her post. Now Mary can actually mention Bob in her next comment on her post.

There are also exceptions where users who aren't shared can still see each other in the mention dropdown list. For example, Sue has interacted with Edgar in Chatter (by liking or commenting on his post or mentioning him). Then you set up user sharing so Sue can't see Edgar. Sue posts on a public Chatter group. She can mention Edgar because, due to their previous interaction, his name shows up on the mention dropdown list. However, if Sue clicks the Edgar mention, she gets an error because, due to user sharing, she can't see him.

SEE ALSO:

[User Sharing](#)

Report Types Support for User Sharing

Reports based on standard report types might expose data of users to whom a user doesn't have access.

The following report types might expose data of users to whom a viewing user doesn't have access.

- Accounts
- Account Owners
- Accounts with Assets
- Accounts with Custom Objects
- Accounts with Partners
- API Usage
- Campaigns with Opportunities
- Custom Object Opportunity with Quotes Report
- Events with Invitees
- Opportunity
- Opportunity Field History
- Opportunity History
- Opportunity Trends
- Opportunities and Connections
- Opportunities with Competitors
- Opportunities with Contact Roles
- Opportunities with Contact Roles and Products

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

- Opportunities with Custom Objects
- Opportunities with Partners
- Opportunities with Products
- Opportunities with Products and Schedules
- Opportunities with Quotes and Quote Documents
- Opportunities with Quotes and Quote Line Items
- Opportunities with Sales Teams
- Opportunities with Sales Teams and Products
- Split Opportunities
- Split Opportunities with Products
- Split Opportunities with Products and Schedules

By default, these reports are accessible only to users who have the appropriate access. However, you can change the setting such that users without the appropriate access to the relevant users can see those reports.

Additionally, some reports may display a user's role. When a user can see a record but does not have access to the record owner, the user can see the owner's role on those reports.

SEE ALSO:

[Control Standard Report Visibility](#)

Differences Between User Sharing with Manual Sharing and Sharing Sets

Manual sharing and sharing sets provide access to different groups of users.

You can control who sees whom in the organization, including internal and external users, if your organization has User Sharing enabled. Manual sharing and sharing sets provide additional access beyond the organization-wide defaults and sharing rules. Some external users, such as high-volume Experience Cloud site users, don't have roles and can't be used in sharing rules.



Example: Grant internal and most external users access to a user by creating a manual share using the Sharing button on the user detail page of that user. Grant high-volume users access to other users by creating a sharing set.

The following table shows when to use manual sharing and sharing sets.

	Users Getting Access		
	Internal	External (Non-high-volume users)	High-volume users
Internal	Manual Sharing	Manual Sharing	Sharing Set
External (Non-high-volume users)	Manual Sharing	Manual Sharing	Sharing Set

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Manual sharing available in: Salesforce Classic

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Users Getting Access

High-volume users	Manual Sharing	Manual Sharing	Sharing Set
--------------------------	----------------	----------------	-------------

SEE ALSO:

[User Sharing](#)

Manage Additional Sharing Settings

Besides configuring the organization-wide defaults and sharing rules, you can configure the following items on the Sharing Settings Setup page.

- [Control standard report visibility.](#)
- [Control manual sharing for user records.](#)
- [Control how users can share records with their managers and manager subordinates groups.](#)
- [Control who community or portal users can see.](#)
- [Control guest users' sharing settings.](#)
- [Control site user access to cases.](#)
- [Control whether to use a person role for the first site user in partner and customer accounts.](#)
- [Control who can view record names in lookup and system fields.](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#))

Available in: **Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

[Control Manual Sharing for User Records](#)

Enable or prevent users from sharing their own user records with other users across the organization.

[Control Standard Report Visibility](#)

Show or hide standard reports that might expose data of users to whom a user doesn't have access.

[Require Permission to View Record Names in Lookup Fields](#)

To better protect your Salesforce org's data, you can restrict who can view record names in lookup fields and system fields, such as Created By and Last Modified By. If you enable the Require permission to view record Names in lookup fields setting, users must have Read access to these records or the View All Lookup Record Names permission to view this data.

Control Manual Sharing for User Records

Enable or prevent users from sharing their own user records with other users across the organization.

You can control whether the Sharing button is displayed on user detail pages. This button enables a user to grant others access to the user's own user record. You can hide or display this button for all users by following these steps.

1. From Setup, in the Quick find box, enter *Sharing Settings*, then select **Sharing Settings**.
2. Click **Edit** in the Organization-Wide Defaults area.
3. Select the **Manual User Record Sharing** checkbox to display the Sharing button on user detail pages, which enables users to share their records with others. Or deselect the checkbox to hide the button, which prevents users from sharing their user records with others.
4. Click **Save**.

When the organization-wide default for users is set to Public Read Only, users get read access to all other user records, can see those users in search and list views, and can interact with those users on Chatter and Experience Builder sites.

 **Example:** For example, a partner user wants to collaborate with the sales representative in a community or forum. If you've disabled the *Site User Visibility* checkbox in the Sharing Settings page, site users can only be seen by themselves and their superiors in the role hierarchy. You can use manual sharing to grant the partner user read access to the sales representative by using the Sharing button on the sales representative's user detail page. This access enables both parties to interact and collaborate in sites.

SEE ALSO:

[Control Which Users Experience Cloud Site Users Can See](#)

Control Standard Report Visibility

Show or hide standard reports that might expose data of users to whom a user doesn't have access.

You can control whether users can see reports based on standard report types that can expose data of users to whom they don't have access. When User Sharing is first enabled, all reports that contain data of users to whom a viewing user doesn't have access are hidden.

1. From Setup, in the Quick Find box, enter *Sharing Settings*, then select **Sharing Settings**.
2. Click **Edit** in the Organization-Wide Defaults area.
3. To allow users to view reports based on standard report types that can expose data of users to whom they don't have access, select the **Standard Report Visibility** checkbox. Or, to hide these reports, deselect this checkbox.
4. Click **Save**.

Notes about visibility:

- If the organization-wide default for the user object is Private and the **Standard Report Visibility** checkbox is selected, a person viewing the report can see the names of users that are listed in the report. To see details such as username and email address, the viewer must have access to the users.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To enable or disable manual user record sharing:

- [Manage Users](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To set standard report visibility:

- [Manage Sharing](#)

- When you deselect the **Standard Report Visibility** checkbox, users with the “View All Users” permission can still see all reports based on standard report types. All users can also see these reports if the organization-wide default for the user object is Public Read Only.
- If the organization-wide default for the user object is Public, the data that is exposed in standard report types includes data from fields on records that other users own. All information from the secondary records is exposed, including information that isn’t directly related to the current user. For example, if user object sharing is set to Public, the standard Accounts with Assets report exposes user data from the Accounts object and the Assets object.
- Visibility behavior also differs for standard and custom report types:
 - Standard Report types operate on the primary object's sharing settings. For example, the Accounts and Assets standard report type respects only the Accounts sharing settings.
 - Custom Report Types respect both primary and secondary object sharing. For example, the Accounts and Assets custom report types respect the sharing settings of both Accounts and Assets.

Important: When Analytics sharing is in effect, all users in the organization get Viewer access to report and dashboard folders that are shared with them. Users who have been designated Manager or Editor on a folder, and users with extra administrative permissions, can have more access. Each user’s access to folders is based on the combination of folder access and user permissions. To ensure that standard report folders are hidden as needed, remove sharing for all users from the folders. Then deselect the **View Dashboards in Public Folders** and **View Reports in Public Folders** checkboxes for the users’ profiles.

SEE ALSO:

[User Sharing](#)

[Report Types Support for User Sharing](#)

Require Permission to View Record Names in Lookup Fields

To better protect your Salesforce org’s data, you can restrict who can view record names in lookup fields and system fields, such as Created By and Last Modified By. If you enable the Require permission to view record Names in lookup fields setting, users must have Read access to these records or the View All Lookup Record Names permission to view this data.

1. From Setup, in the Quick Find box, enter *Sharing Settings*, and then select **Sharing Settings**.
2. Click **Edit** in the Organization-Wide Defaults area.
3. Select **Require permission to view record names in lookup fields**.
4. Enable the View All Lookup Record Name permission in custom profiles or permission sets for users who must see record names in all lookup and system fields, regardless of sharing settings.

Note: The View All Lookup Record Name permission only applies to lookup record names in list views and record detail pages.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

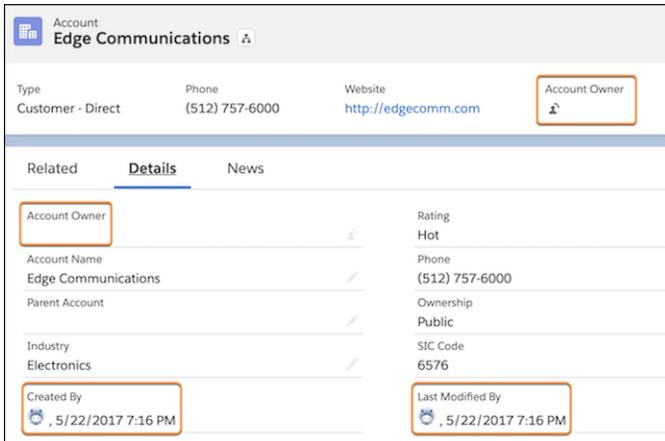
Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To modify sharing settings:

- [Manage Sharing](#)

 **Example:** After the Require permission to view record names in lookup fields setting is enabled, in Lightning Experience, users who don't have Read access or the View All Lookup Record Names permission see the lookup field labels, but not the data in the fields.



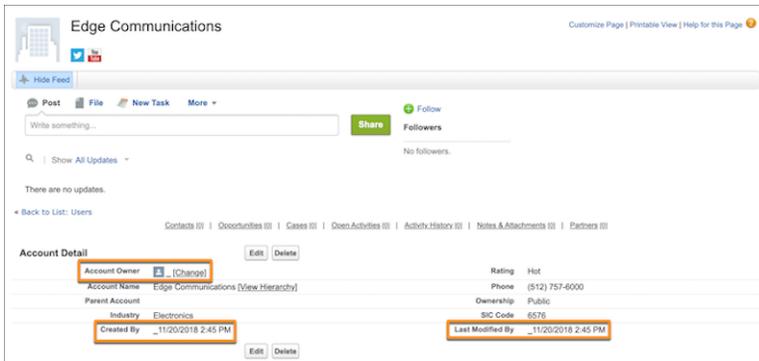
Account
Edge Communications

Type: Customer - Direct | Phone: (512) 757-6000 | Website: http://edgecomm.com | Account Owner

Related | **Details** | News

Account Owner	Rating: Hot
Account Name: Edge Communications	Phone: (512) 757-6000
Parent Account	Ownership: Public
Industry: Electronics	SIC Code: 6576
Created By: [User], 5/22/2017 7:16 PM	Last Modified By: [User], 5/22/2017 7:16 PM

In Salesforce Classic, users who don't have Read access or the View All Lookup Record Names permission see an underscore in system user lookup fields. They also see the record ID in custom user lookup and non-user lookup fields.



Edge Communications

Account Detail

Account Owner: [User] (Change)	Rating: Hot
Account Name: Edge Communications (View Hierarchy)	Phone: (512) 757-6000
Parent Account	Ownership: Public
Industry: Electronics	SIC Code: 6576
Created By: [User], 11/20/2018 2:45 PM	Last Modified By: [User], 11/20/2018 2:45 PM

 **Note:** In Lightning Experience, a parent record's name is visible in lookup fields if the user has access to its child record via a "View All" permission. This behavior applies even if the user doesn't have access to the parent record. In Salesforce Classic, the parent record's ID is displayed instead of its name.

SEE ALSO:

["View All" and "Modify All" Permissions Overview](#)

View Sharing Overrides

When you select an object in the Sharing Settings page, the page includes a Sharing Overrides related list, which shows any profiles that ignore sharing settings for that object.

 **Note:** The Sharing Overrides list doesn't show permissions granted through permission sets, which may also override sharing settings for an object.

1. From Setup, in the Quick Find box, enter *Sharing Settings*, and then select **Sharing Settings**.
2. Select an object from the Manage Sharing Settings For list.

For each profile, the list specifies the permissions that allow it to override sharing settings. The "View All Data" and "Modify All Data" permissions override sharing settings for all objects in the organization, while the object permissions "View All" and "Modify All" override sharing settings for the named object.

To override sharing settings for specific objects, you can create or edit permission sets or profiles and enable the "View All" and "Modify All" object permissions. These permissions provide access to all records associated with an object across the organization, regardless of the sharing settings. Before setting these permissions, compare the different ways to control data access.

SEE ALSO:

[Profiles](#)

Built-in Sharing Behavior

Salesforce provides implicit sharing between accounts and child records (opportunities, cases, and contacts), and for various groups of site and portal users.

Built-in sharing behaviors apply only to standard relationships.

Sharing between accounts and child records

- Access to a parent account—If you have access to an account's child record, you have implicit Read Only access to that account.
- Access to child records—If you have access to a parent account, you have access to the associated child records. The account owner's role determines the level of access to child records.

Sharing behavior for site or portal users

- Account and contact access—An account's portal or site user has Read Only access to the parent account and to all of the account's contacts.
- Management access to data owned by Service Cloud portal users—Since Service Cloud portal users don't have roles, portal account owners can't access their data via the role hierarchy. To grant them access to this data, you can add account owners to the portal's share group where the Service Cloud portal users are working. This step provides access to all data owned by Service Cloud portal users in that portal.
- Case access—If a portal or site user is a contact on a case, then the user has Read and Write access on the case.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To view sharing overrides:

- [View Setup and Configuration](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Sharing for accounts and contacts is available in: **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

Sharing for cases and opportunities is available in **Enterprise, Performance, Unlimited,** and **Developer** Editions

Group membership operations and sharing recalculation

Simple operations such as changing a user's role, moving a role to another branch in the hierarchy, or changing a site or portal account's owner can trigger a recalculation of sharing rules. Salesforce must check access to user's data for people who are above the user's new or old role in the hierarchy, and either add or remove shares to any affected records.

 **Note:** These sharing behaviors simplify administration for data access but can make mass inserts and mass updates slow. For best practices on designing record access in a large organization, see [Designing Record Access for Enterprise Scale](#).

SEE ALSO:

[Control Who Sees What](#)

Object-Specific Share Locks

When you create, edit, or delete a sharing rule, recalculation runs to update record access in your Salesforce org. This operation can take some time if you have many users and records. The object-specific share locks feature enables you to make changes to a sharing rule for other objects simultaneously, depending on the objects affected by the sharing rules, sharing rule type, and target groups or roles of the affected users.

Without object-specific share locks, you can't submit simultaneous sharing changes until recalculation across all objects is complete. Review the following behavior considerations for object-specific share locks.

Criteria-based and owner-based sharing rules

Recalculation is run if a sharing rule has changed or when you click the **Recalculate** button on the Sharing Settings page. Clicking this button locks sharing rules for that object (1), but you can still make changes to sharing rules for another object.

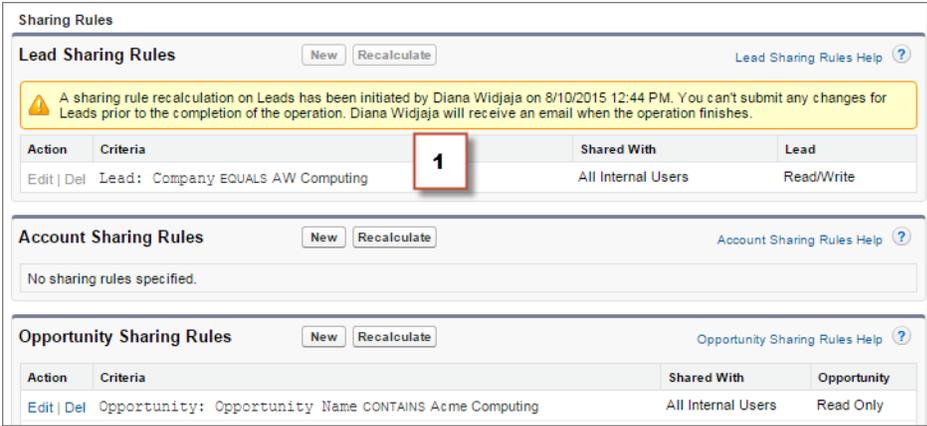
 **Note:** Use the Recalculate buttons on the Sharing Rules related lists only if sharing rule updates have failed or aren't working as expected.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

See [Sharing Rule Considerations](#) for more information on availability.



Action	Criteria	Shared With	Lead
Edit Del	Lead: Company EQUALS AW Computing	All Internal Users	Read/Write

Action	Criteria	Shared With	Opportunity
Edit Del	Opportunity: Opportunity Name CONTAINS Acme Computing	All Internal Users	Read Only

When recalculation for an owner-based sharing rule is in progress, you can't create, edit, or delete owner-based sharing rules for that object targeting the same group of users. For example, let's say you're creating an owner-based lead sharing rule targeting the All Internal Users group. While recalculation is in progress, you can create another owner-based sharing rule for leads targeting any other public group except the All Internal Users group. You can create, update, or delete owner-based sharing rules for leads targeting all internal users only after the recalculation finishes. You receive an email notification when the recalculation is complete.

When recalculation for a criteria-based sharing rule is in progress, you can't edit or delete that rule. But you can create, edit, or delete any other criteria-based or owner-based sharing rule for that object regardless of the target group of users.

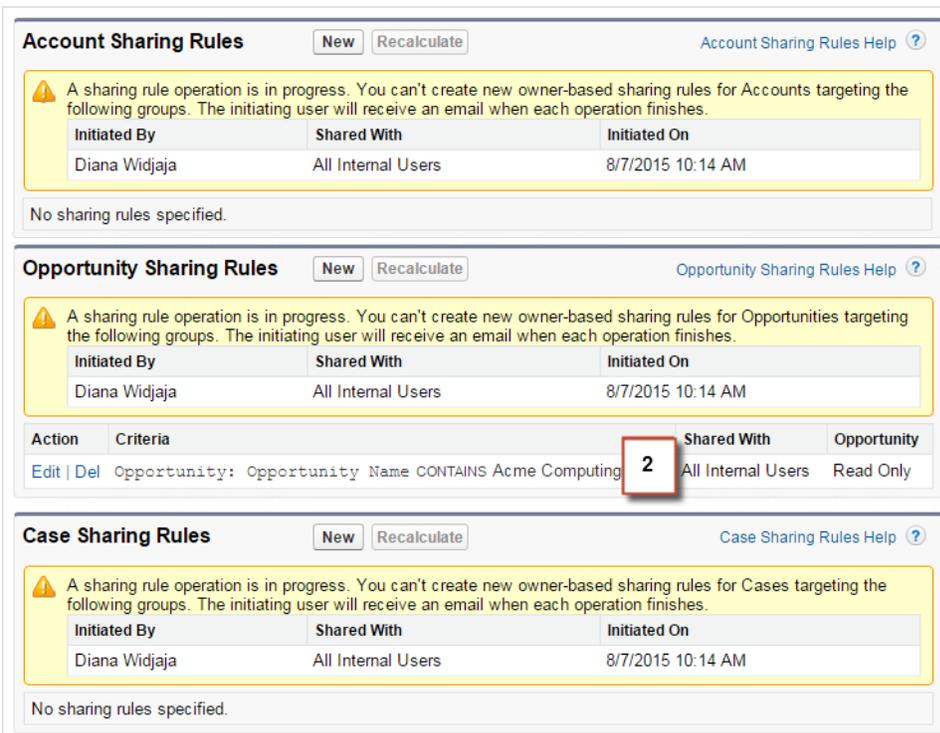
 **Note:** You can't modify the org-wide defaults when a sharing rule recalculation for any object is in progress. Similarly, you can't modify sharing rules when recalculation for an org-wide default update is in progress.

Account, cases, contacts, and opportunities

Sharing rules can affect accounts and the associated account children—cases, contacts, and opportunities—so they're locked together to ensure that recalculation runs properly. For example, creating or editing an account sharing rule prevents you from creating or editing a case, contact, or opportunity sharing rule. Similarly, creating or editing an opportunity sharing rule prevents you from creating or editing a case, contact, or account sharing rule before recalculation is complete. Locks aren't shared across objects, except across accounts and associated account children.

 **Note:** Clicking the Recalculate button for any of these four objects' sharing rules prevents anyone from making changes to sharing rules for those objects until recalculation finishes.

In the following example, an owner-based account sharing rule has been deleted and recalculation is in progress. Although you can't create, edit, or delete another ownership-based sharing rule for any of these objects, you can make changes to a criteria-based sharing rule (2) for those objects.



The screenshot displays three sections of sharing rules: Account Sharing Rules, Opportunity Sharing Rules, and Case Sharing Rules. Each section has a 'New' and 'Recalculate' button and a help link. A yellow warning banner is present in each section, stating: 'A sharing rule operation is in progress. You can't create new owner-based sharing rules for [Object] targeting the following groups. The initiating user will receive an email when each operation finishes.' Below the banner is a table with columns: Initiated By, Shared With, and Initiated On. The data in all three sections is: Initiated By: Diana Widjaja, Shared With: All Internal Users, Initiated On: 8/7/2015 10:14 AM. Below the Opportunity Sharing Rules section is a table with columns: Action, Criteria, Shared With, and Opportunity. The data row is: Edit | Del, Opportunity: Opportunity Name CONTAINS Acme Computing, 2, All Internal Users, Read Only. The number '2' is highlighted with a red box.

SEE ALSO:

[Sharing Rules](#)

[Recalculate Sharing Rules Manually](#)

[Defer Sharing Calculations](#)

Managing Folders

USER PERMISSIONS

To create, edit, or delete public document folders:	Manage Public Documents
To create, edit, and delete public email template folders in Salesforce Classic:	Manage Public Classic Email Templates (in Salesforce Classic only)
To create, edit, and delete public email templates in Lightning Experience:	Manage Public Lightning Email Templates (in Lightning Experience only)
To create, edit, and delete enhanced email template folders in Lightning Experience:	Create Folders for Lightning Email Templates
To create, edit, and delete public report folders:	Manage Reports in Public Folders
To create, edit, and delete public dashboard folders:	Manage Dashboards AND View All Data

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions except **Database.com**

Report folders not available in: **Contact Manager, Essentials, Group, and Personal** Editions

A folder is a place where you can store reports, dashboards, documents, or email templates. Folders can be public, hidden, or shared, and can be set to read-only or read/write. You control who has access to its contents based on roles, permissions, public groups, and license types. You can make a folder available to your entire organization, or make it private so that only the owner has access.

- To access [report and dashboard folders](#), click the Reports or Dashboards tab.
- To access [document folders](#) in Salesforce Classic, click the **Documents** tab.
- To access [library folders](#) in Lightning Experience, click the **Files** tab, and then click **Libraries**.
- To access [Classic email template folders](#), from Setup, in the Quick Find box, enter *Classic Email Templates*, then select **Classic Email Templates**.
- To access [Lightning email template folders](#), click the **Email Templates** tab.

Considerations

You can modify the contents of a folder only if the folder access level is set to read/write. Only users with the “Manage Public Documents” or “Manage Public Templates” permission can delete or change a read-only folder. Regardless of permissions or folder settings, users can’t edit unfiled or personal folders. Users with the “Manage Reports in Public Folders” permission can edit all reports in public folders but not reports in other users’ personal folders.

Lightning Experience Email Template Folders

- Admins and users with the Modify All Data permission can read, edit, clone, and delete email templates in other users’ private folders.
- To edit enhanced folders, enhanced folders must be enabled and the folder itself must have editing permissions.

SEE ALSO:

[Create and Edit Folders](#)

[Moving Documents and Email Templates in Folders](#)

Create and Edit Folders

Create document and email template folders and set their visibility so that users have the correct access level.

This topic describes how to create document and email template folders and set their visibility in Salesforce Classic.

- For information on report or dashboard folders, see [Report and Dashboard Folders](#).
- For information on folder sharing for email templates in Lightning Experience, see [Enable Folders and Enhanced Sharing for Email Templates](#).
- For information on creating library folders in Lightning Experience, see [Create Folders in Libraries in Lightning Experience](#).

Click **Create New Folder** or **Edit** from the Documents tab or the Classic Email Templates Setup page.

1. Enter a `Folder Label`. The label is used to refer to the folder on user interface pages.
2. Choose a `Public Folder Access` option. Select read/write if you want users to be able to change the folder contents. A read-only folder can be visible to users but they can't change its contents.
3. Select an email template and click **Add** to store it in the new folder. Skip this step for document folders.
4. Choose a folder visibility option:
 - `This folder is accessible by all users, including portal users` gives folder access to all users in your organization, including portal users.
 - `This folder is accessible by all users, except for portal users` gives folder access to all users in your organization, but denies access to portal users. This option is only available for report and dashboard folders in organizations with a partner portal or Customer Portal enabled. If you don't have a portal, you won't see it.
 - `This folder is hidden from all users` makes the folder private.
 - `This folder is accessible only by the following users` allows you to grant access to a desired set of users. The sets of users vary by edition and whether your organization has territory management. Choose a set of users from the `Search` dropdown list. Then select the desired value from the `Available for Sharing` list and click **Add** to move the value to the `Shared To` list.

When you share a folder with a group, managers of the group members have no access to the folder unless those managers are also members of the group.

5. Click **Save**.

SEE ALSO:

[Managing Folders](#)

[Considerations for Using Public and Private Email Templates in Lightning Experience](#)

[Considerations for Email Template Folders and Sharing](#)

EDITIONS

Available in: both Salesforce Classic (**not available in all orgs**) and Lightning Experience

Available in: all editions except **Database.com**

Report folders not available in: **Contact Manager, Essentials, Group, and Personal** Editions

USER PERMISSIONS

To create, edit, or delete public document folders:

- `Manage Public Documents`

To create, edit, and delete public email template folders in Salesforce Classic:

- `Manage Public Classic Email Templates (in Salesforce Classic only)`

Moving Documents and Email Templates in Folders

You can move documents or email templates to a different folder.

1. Select the item to be stored in a folder.
2. For documents, click **Edit Properties**. For email templates, click **Edit**.
3. Choose another folder.
4. Click **Save**.

Just like email template folders contain email templates, document folders can only contain documents. To store an attachment in a document folder, save the attachment to your computer and upload it to the document library.

 **Note:** Email templates that are used by Web-to-Case, Web-to-Lead, assignment rules, or escalation rules must be marked as “Available for Use.”

For information on moving reports and dashboards in folders, see [Move Reports Between Folders in Lightning Experience](#) and [Move Dashboards Between Folders in Lightning Experience](#).

SEE ALSO:

[Managing Folders](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions except **Database.com**

Report folders not available in: **Contact Manager, Essentials, Group,** and **Personal** Editions

USER PERMISSIONS

To create, edit, or delete public document folders:

- Manage Public Documents

To create, edit, and delete public email template folders in Salesforce Classic:

- Manage Public Classic Email Templates (in Salesforce Classic only)

To create, edit, and delete public email templates in Lightning Experience:

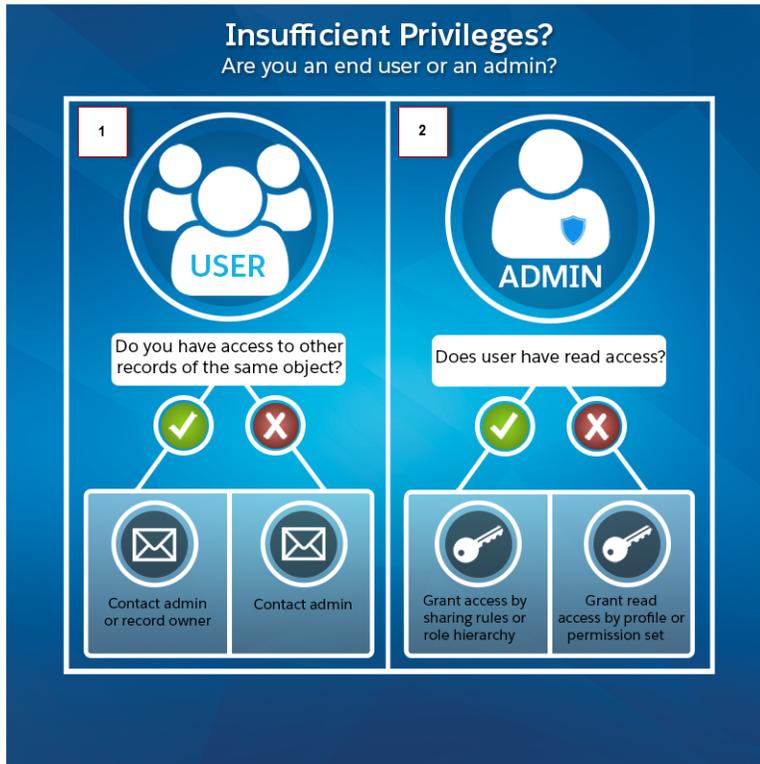
- Manage Public Lightning Email Templates (in Lightning Experience only)

To create, edit, and delete enhanced email template folders in Lightning Experience:

- Create Folders for Lightning Email Templates

Insufficient Privileges Errors

Follow this troubleshooting flowchart if you're encountering an insufficient privileges error.



EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions**

You can obtain access to a record or object by contacting your Salesforce org's admin or the record owner of the record you're trying to access. How you contact your admin depends on your company's internal business policies and practices.

If you're a user (1), determine if you have access to other records of the same object.

- Have access to other records of the same object: For example, you have access to account record A but not account record B. Contact your Salesforce admin or the record owner to request access.
- Don't have access to other records of the same object: Contact your Salesforce admin to request access.

If you're an admin (2), determine if the user has read access to the record.

- Have read access: Grant more access using sharing mechanisms such as sharing rules, manual sharing, or sharing sets. Also, the **Sharing** button on the record detail page can grant users record access on a one-time basis and gives you the flexibility to remove that access later.
- Don't have read access: Grant read access using a profile or permission set.

If you must share a report or dashboard folder, share the folder it's in. Recall that when you create a folder, only you and users with administrative permissions can see it.

For more information, see [Resolving Insufficient Privileges Errors](#).

[Resolve Permission and Object-Level Access Errors](#)

Missing or incorrect object and user permissions can cause Insufficient Privileges errors. You can troubleshoot this type of error by checking profile and permission sets.

[Resolve Record-Level Access Errors](#)

When your sharing settings, such as roles or sharing rules, don't provide enough access, your users can get Insufficient Privileges errors.

[Resolve Process-Level Access Errors](#)

Validation rules can cause Insufficient Privileges errors.

SEE ALSO:

[Sharing Rules](#)[Manual Sharing](#)[Share a Report or Dashboard Folder in Salesforce Classic](#)

Resolving Insufficient Privileges Errors

If you can't access a record or perform a task, like run a report, you most likely don't have the required permission or sharing setting.

You see the Insufficient Privileges error if you don't have the right access on different levels. For example, your profile prevents you from accessing the account object, or your role prevents you from accessing a case record. You also see an Insufficient Privileges error when you click a link to a record or a Visualforce page tab to which you don't have access.

Record owners can resolve most cases by using the Sharing button on the record detail page, which enables them to share the record to another user. Salesforce admins can also resolve this issue using the API, such as querying the [UserRecordAccess](#) object to check a user's access to a set of records. For more information, see the *REST API Developer Guide* and the *SOAP API Developer Guide*.

If these tools can't help you resolve the issue, your Salesforce org's admin can try to diagnose it with these troubleshooting flows.

- [Resolve object-level access errors by reviewing the user profiles and permission sets.](#)
- [Resolve record-level access errors by reviewing the sharing settings, such as organization-wide defaults and sharing rules.](#)
- [Resolve process-level errors by reviewing validation rules.](#)

It's a good idea for an admin to log in to the application using your login to help you resolve an issue.

 **Note:** Watch this video series to understand how to grant users the access they need.  [Who Sees What: Overview \(English only\)](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions**

Resolve Permission and Object-Level Access Errors

Missing or incorrect object and user permissions can cause Insufficient Privileges errors. You can troubleshoot this type of error by checking profile and permission sets.

Generally, the best method for investigating object and permission access issues is through the API. However, you can use the following steps to investigate via point-and-click tools. You can also use the [User Access and Permissions Assistant](#) to help you analyze permission assignments.

1. Verify the object permissions in the user's profile.

Object permissions, configured on profiles and permission sets, determine which objects a user can read, create, edit, or delete.

a. On the user detail page, click the user's profile.

b. On the profile overview page, go to **Object Settings** or **Object Permissions**.

Note the permissions for the object. If the user is trying to view an account, check that the Read permission for the account and contact objects on the user profile is enabled.

If the user is trying to run a report, check that the user has the Read permission on an object that the report references.

2. Verify the user permissions in one of the following ways, depending on your profile user interface.

Note the relevant user permissions. For example, if the user is trying to send an email to a lead, check that the Send Email permission is enabled.

- From the enhanced profile user interface, review the permissions in the App Permissions and System Permissions sections.

- From the original profile user interface, review the permissions under Administrative Permissions and General User Permissions.

3. Verify the permissions in the user's permission sets.

a. On the user detail page, scroll to the Permission Set Assignments related list and click each permission set.

b. On the permission set overview page, click Object Settings and review the assigned object permissions.

c. Review the user permissions in the App Permissions and System Permissions sections.

d. Repeat these steps for each permission set assigned to the user.

4. If needed, assign the necessary permission using a permission set or by updating the profile. Permission sets provide access on an individual basis. Assign permissions on the user profile *only* if all users of this profile require access. Be sure you're aware of your organization's security policy and act accordingly.

SEE ALSO:

[Resolving Insufficient Privileges Errors](#)

[Permission Sets](#)

[User Permissions and Access](#)

[Profiles](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions**

USER PERMISSIONS

To view profiles and permission sets:

- View Setup and Configuration

To edit object permissions:

- Manage Profiles and Permission Sets

AND

Customize Application

Resolve Record-Level Access Errors

When your sharing settings, such as roles or sharing rules, don't provide enough access, your users can get Insufficient Privileges errors.

To verify if the error is at the record level, follow these steps. You can also use the API to query a user's access to a set of records or use the Insufficient Access event log files through Event Monitoring.

1. From Setup, in the Quick Find box, enter *Users*, and then select **Users**. If your Salesforce org uses roles, check the user's role in relation to the record owner.
For example, users can delete records only if they're the record owner, higher in the role hierarchy than the record owner, or the administrator. Similarly, users always have read access to records whose owners are below them in the role hierarchy, unless **Grant Access Using Hierarchies** is deselected (custom objects only).
2. Verify the role of the user and the role of the user who owns the record. A user can't delete or merge accounts owned by someone in an unrelated role hierarchy, even if the user has the appropriate permissions on the objects.
3. Review your sharing rules. Check that the user is included in the sharing rules.
 - a. From Setup, in the Quick Find box, enter *Sharing Settings*, and then select **Sharing Settings**.
 - b. Check the public group (or other categories such as roles or queues) and verify that the user is included in that sharing rule.
4. From Setup, in the Quick Find box, enter the team that you want to check, such as *Account Teams*, and then select the team. Review your teams to determine if the user is supposed to have access through a team. If your organization uses teams for accounts, opportunities, or cases, verify that you didn't miss the user when you set up the teams. Add the user to the team, if appropriate.
5. Review your manual shares. If the user had access via manual sharing, but lost this access, find out if one of these events occurred:
 - The record owner changed, causing the manual share to be removed.
 - The record owner, an administrator, or a user above the owner in the role hierarchy removed the manual share using the Sharing button on the record detail page.
 - An active restriction rule blocks access to the record because the rule's user criteria includes the user, but the record criteria isn't met.
 - a. In Lightning Experience, click **Sharing Hierarchy** from the Action Menu on the record. In Salesforce Classic, click **Sharing** on the record, then click **Expand List**. The Sharing Hierarchy page shows the users, groups, roles, and territories that have access to the record. In Lightning, clicking **View** shows reasons for access, including the name of the sharing mechanism that grants access. If a restriction rule blocks access to the record, a message is shown to confirm that access is blocked.
 - b. If the user must gain access via a manual share, create a manual share using the Sharing button on the record.
6. Review your territories. If your organization is using territories, check that the user is included in the territories, and the record is under the correct territory where the user is a member.
7. Review your sharing sets and share groups. If your organization is using sharing sets to grant access to external users or share groups to share records owned by high-volume Experience Cloud site users, check that the profile of the user is included in the sharing set, and that the user is added to the share group.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions**

USER PERMISSIONS

To create or edit sharing rules:

- Manage Sharing

To set up teams:

- Customize Application

To manage territories:

- Manage Territories

In Lightning Experience, manual sharing isn't available for all objects. Find the list of available objects in [Manual Sharing Considerations](#).

SEE ALSO:

[Resolving Insufficient Privileges Errors](#)

[Create a User Role](#)

[Sharing Rules](#)

[Create a Sharing Set](#)

[Use Share Groups to Share Records Owned by High-Volume Experience Cloud Site Users](#)

Resolve Process-Level Access Errors

Validation rules can cause Insufficient Privileges errors.

To resolve Insufficient Privileges errors, you typically determine if misconfigured permission sets, profiles, or sharing settings are causing the errors. Another option is to review your organization's validation rules.

1. Review your validation rules.
A validation rule can prevent the user from completing a task, such as transferring a case record after it's closed.
2. From Object Manager, find the object that you want to check, and then scroll down to Validation Rules.
3. Verify that none of the validation rules are causing the error or fix the validation rule.

SEE ALSO:

[Resolving Insufficient Privileges Errors](#)

[Define Validation Rules](#)

Restriction Rules

Restriction rules let you enhance your security by allowing certain users to access only specified records. They prevent users from accessing records that can contain sensitive data or information that isn't essential to their work. Restriction rules filter the records that a user has access to so that they can access only the records that match the criteria you specify.

Watch how you can use restriction rules to further refine user record access.

 [Watch a video](#)

Restriction rules are available for custom objects, external objects, contracts, tasks, and events. You can create up to two active restriction rules per object in Enterprise and Developer editions and up to five active restriction rules per object in Performance and Unlimited editions. Restriction rules are applied to the following Salesforce features:

- List Views
- Lookups
- Related Lists

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions**

USER PERMISSIONS

To view and change validation rules:

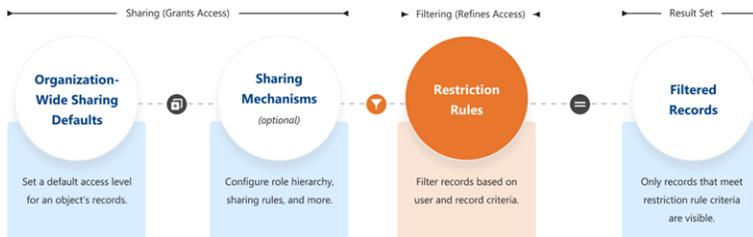
- View Setup and Configuration
- AND
- Customize Application

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise, Performance, Unlimited, and Developer** Editions

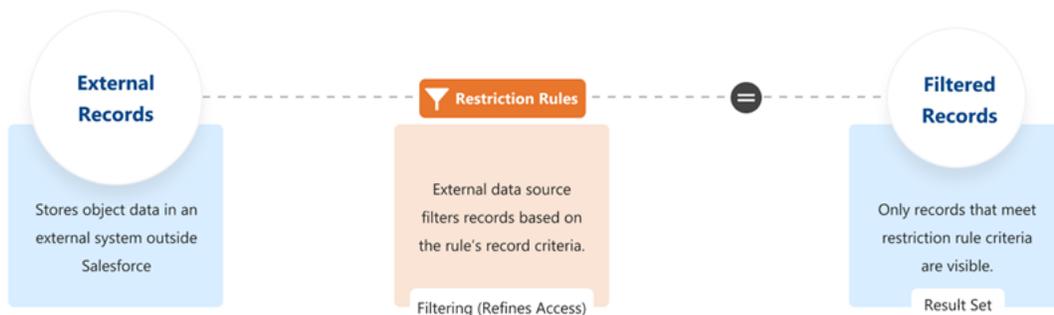
- Reports
- Search
- SOQL
- SOSL



When a restriction rule is applied to a user, the records that the user is granted access to via org-wide defaults, sharing rules, and other sharing mechanisms are filtered by criteria that you specify. For example, if users navigate to the Today's Tasks tab or to a list view for activities, they see only the records that meet the restriction rule's criteria. If a user has a link to a record that is no longer accessible after a restriction rule is applied, the user sees an error message.

Note: Before setting up a restriction rule on an external object, review these considerations.

- Restriction rules for external objects don't include organization-wide defaults or sharing mechanisms.
- Only external objects created using the Salesforce Connect: OData 2.0, OData 4.0, and Cross-Org adapters support restriction rules.
- External objects created using the Cross-Org adapter don't support search or SOSL when a rule is applied to a user. Salesforce returns only search results that match the most recently viewed records.
- Disabling search on external objects is recommended.
- External objects created using the Salesforce Connect: Custom Adapter aren't supported.



When Do I Use Restriction Rules?

Use restriction rules when you want certain users to see only a specific set of records. Restriction rules can simplify controlling access to records with sensitive or confidential information. Access to contracts, tasks, and events can be difficult to make truly private using organization-wide defaults, making restriction rules the best way to configure this visibility.

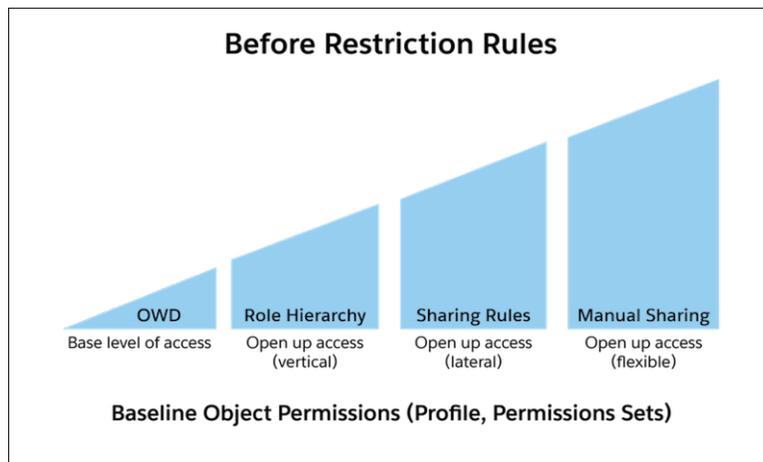
For example, you have competing sales teams that can't see each other's activities, even though these activities are on the same account. With restriction rules, you can make sure that sales teams see only activities that belong to them and are relevant to their work. Or, if you provide confidential services to various individuals, use restriction rules so that only team members responsible for supporting these individuals can see related tasks.

When creating more than one restriction or scoping rule, configure the rules so that only one active rule applies to a given user. Salesforce doesn't validate that only one active rule applies for a given user. If you create two active rules, and both rules apply to a given user, only one of the active rules is observed.

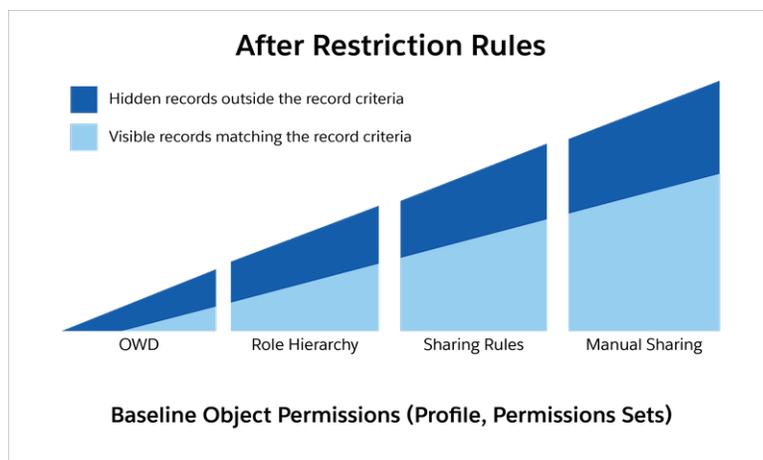
Before creating restriction rules, we recommend that you [Turn Off Salesforce Classic for Your Org](#). Salesforce can't guarantee that restriction rules work as intended for end users who are in the Salesforce Classic experience.

How Do Restriction Rules Affect Other Sharing Settings?

Users get access to records based on your organization-wide defaults and other sharing mechanisms such as sharing rules or enterprise territory management.



When a restriction rule is applied to users, the data that they had read access to via your sharing settings is further scoped to only records matching the record criteria. This behavior is similar to how you can filter results in a list view or report, except that it's permanent. The number of records visible to the user can vary greatly depending on the value that you set in the record criteria.



How Do I Configure Restriction Rules?

You can create and manage restriction rules by navigating to a supported object in the Object Manager. Or use the RestrictionRule Tooling API object or RestrictionRule Metadata API type. For more information on using the API, see the [Restriction Rules Developer Guide](#).

[Create a Restriction Rule](#)

Control the records that a specific user group is permitted to see. When a restriction rule is applied to a user, the data that the user has access to via org-wide defaults, sharing rules, and other sharing mechanisms is filtered by the record criteria that you specify.

[Restriction Rule Considerations](#)

Keep these considerations and limitations in mind while using restriction rules.

[Restriction Rule Example Scenarios](#)

Refer to these sample restriction rules, which fulfill different access requirements.

Create a Restriction Rule

Control the records that a specific user group is permitted to see. When a restriction rule is applied to a user, the data that the user has access to via org-wide defaults, sharing rules, and other sharing mechanisms is filtered by the record criteria that you specify.

Before creating restriction rules, we recommend that you [Turn Off Salesforce Classic for Your Org](#). Salesforce can't guarantee that restriction rules work as intended for end users who are in the Salesforce Classic experience.

Restriction rules are available for custom objects, external objects, contracts, events, tasks, time sheets, and time sheet entries. You can create up to two restriction rules per object in Enterprise and Developer editions and up to five restriction rules per object in Performance and Unlimited editions.

Only external objects created using the Salesforce Connect: OData 2.0, OData 4.0, and Cross-Org adapters support restriction rules. Find out more in [Restriction Rule Considerations](#).

1. In the Object Manager, click the object you want to create a restriction rule on.
 - a. For an external object, enter *External Data Sources* in the Quick Find box in Setup, then select **External Data Sources**. Select an external object from the related list on this page.
2. In the sidebar, click **Restriction Rule**, and then click **Create a Rule**.
3. Enter the rule's name and full name. The full name is the name of the component used by the API.
4. To have the rule take effect upon saving, select **Active**.
5. Under User Criteria, select which users this restriction rule applies to.
 - If the rule applies to a subset of users such as those in a given role, profile, or department, select **User Criteria**. Then, select the field to use as criteria.
Set the Type field as **Current User** when the rule applies to the currently logged-in user.
 - If the rule applies to a subset of users with a custom permission, select **Permission Criteria**.
To filter records for users with the custom permission, set the Boolean value to **True**. To filter records for users who don't have the custom permission, set the Boolean value to **False**.
6. Under Record Criteria, select which records the specified users are allowed to see. For the Field value, you can reference another object's field using dot notation.
To designate more than one value in the record criteria, you can specify a list of comma-separated strings or 15-character IDs in the Value field.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To create and manage restriction rules:

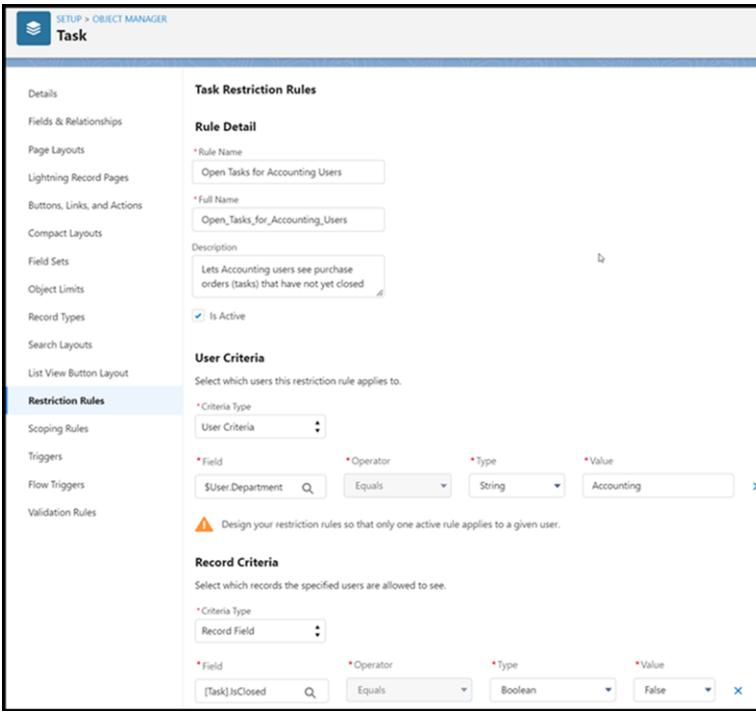
- Manage Sharing

To view restriction rules:

- View Setup & Configuration AND View Restriction and Scoping Rules

 **Tip:** To include a single value that contains a comma, surround the value with double quotes ("").

7. Save the rule.



Task Restriction Rules

Rule Detail

* Rule Name: Open Tasks for Accounting Users

* Full Name: Open_Tasks_for_Accounting_Users

Description: Lets Accounting users see purchase orders (tasks) that have not yet closed

Is Active

User Criteria

Select which users this restriction rule applies to.

* Criteria Type: User Criteria

* Field: \$User.Department * Operator: Equals * Type: String * Value: Accounting

⚠ Design your restriction rules so that only one active rule applies to a given user.

Record Criteria

Select which records the specified users are allowed to see.

* Criteria Type: Record Field

* Field: [Task].IsClosed * Operator: Equals * Type: Boolean * Value: False

 **Note:** Salesforce doesn't validate that only one active rule applies for a given user. If you create two active rules, and both rules apply to a given user, only one of the active rules is observed. In this case, records that the user shouldn't have access to could be accessible.

SEE ALSO:

- [Enable Custom Permissions in Permission Sets](#)
- [Restriction Rule Considerations](#)

Restriction Rule Considerations

Keep these considerations and limitations in mind while using restriction rules.

Available Objects

- Before creating restriction rules, we recommend that you [Turn Off Salesforce Classic for Your Org](#). Salesforce can't guarantee that restriction rules work as intended for end users who are in the Salesforce Classic experience.
- Restriction rules are available for custom objects, external objects, contracts, events, tasks, time sheets, and time sheet entries.
- In calendars, if the Show Details access level is selected, users can see the subject of all events, regardless of the restriction rules created. For more information, see [Share Your Calendar in Lightning Experience](#) in Salesforce Help.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise, Performance, Unlimited, and Developer** Editions

Applicable Features

- Restriction rules are applied to the following Salesforce features:
 - List Views
 - Lookups
 - Related Lists
 - Reports
 - Search
 - SOQL
 - SOSL
- Restriction rules support custom picklist values in record and user criteria. If you delete a custom picklist value used in a restriction rule, the rule no longer works as intended.
- Use the Activity Timeline instead of activity related lists, such as Open Activities or Activity History. If you use activity related lists, create rules on task or event objects using fields that are only available in the related lists.
- If you use Open Activities and Activity History related lists, when restriction rules are applied, it's possible that fewer than 50 records are displayed when more activities exist that the user has access to. This behavior occurs because these lists display at most 50 records, and restriction rules are applied after. This behavior is related to the known issue, [Limit of Fifty Records Visible in Related List View](#).
- After restriction rules are applied, users can still see records that they previously had access to in the search box shortcuts list or in the Recently Viewed list view. When users click the record name, they can't access the record and get an error.
- Users can see their subordinates' events in calendars even if the users have an active restriction rule applied.
- If a user creates an event or a task record using the Chatter publisher, the record name is visible in the related Chatter post. Restriction rules don't restrict visibility to these record names.
- Users can't clone records that have a lookup to a record that they can't see due to a restriction rule. For example, you have a restriction rule that prevents a user from seeing a specific contract record, and the user tries to clone an order record that has a lookup to the contract record. The user gets an error, preventing the clone operation from succeeding.
- Restriction rules aren't applied for code executed in System Mode.
- Users with the View All or View All Data permissions can view all records regardless of restriction rules. Users with the Modify All or Modify All Data permissions can view, edit, and delete all records regardless of restriction rules.
- A user with a restriction rule applied might not find all possible matching results when searching for a record. For performance reasons, search crowding applies limits to the number of search results. The record the user is looking for can fall outside those limits. Learn how to adjust your searches for the best results at [How Search Crowding Affects Search Results](#).
- The `UserRecordAccess` object doesn't consider whether a user's access is blocked due to a restriction rule. If a user's access is blocked even though query results state that they should have access, check to see if a restriction rule on the object prevents the user's access.

Creating Restriction Rules

- You can create up to two restriction rules per object in Enterprise and Developer editions and up to five restriction rules per object in Performance and Unlimited editions.
- Create only one restriction or scoping rule per object per user. In other words, for a given object, only one restriction or scoping rule at most can have the User Criteria field evaluate to `true` for a given user.
- Creating a restriction rule for an object doesn't automatically restrict access to its child objects. For example, if you create a restriction rule for the Contract object, the access doesn't change for notes that are associated with the affected contract records. To secure these child objects, you must use other sharing mechanisms.

- You can reference another object's field using the Record Criteria field. See [Restriction Rule Example Scenarios](#) for examples.
- In the rule's record criteria, you can't reference fields on the object's parent. For example, if you're creating a rule for the Task object, the record criteria can't reference a field on the parent Activity object.
- We support these data types in the User Criteria and Record Criteria fields:
 - boolean
 - date
 - dateTime
 - double
 - int
 - reference
 - string
 - time
 - single picklist



Note: Comma-separated ID or string values are supported in the Record Criteria field.

- Restriction rules support only the EQUALS operator. The use of AND and OR operators isn't supported.
- The use of formulas isn't supported.
- Don't create rules on Event.IsGroupEvent, which indicates whether the event has invitees.
- You can use a change set or unlocked package to move restriction rules from one org to another.
- Some IDs are specific to your Salesforce org, such as role, record type, or profile IDs. If you include these IDs in your User Criteria or Record Criteria fields, keep this consideration in mind when deploying rules between sandboxes or to a production org. You must modify these IDs in the target org if the restriction rules were originally created somewhere else.
- When you reference the Owner field, you must specify the object type in your syntax. For example, the Owner field on an Event object can contain a user or a queue, but queues aren't supported in restriction rules. So it's necessary to specify Owner:User in the record criteria syntax when the criteria should allow only users.

Restriction Rules and External Objects

- Only external objects created using the Salesforce Connect: OData 2.0, OData 4.0, and Cross-Org adapters support restriction rules.
- External objects created using the Cross-Org adapter don't support search or SOSL when a rule is applied to a user. Salesforce returns only search results that match the most recently viewed records.
- External objects created using the Salesforce Connect custom adapter aren't supported.
- External object record data is stored outside Salesforce. Admins are responsible for ensuring that rules they create on external objects don't negatively impact performance in Salesforce or in the external system.



Important:

- Editing or deleting a restriction rule on an external object causes an additional database call, which can result in additional billing when the external data source bills per call.
- When search is enabled for external object records, searching requires additional database calls each time. Avoid additional charges by turning off search for external object records.

As with all restriction rules, using only object fields that are indexed is recommended, especially in record criteria.

- Using external IDs in record criteria isn't recommended.
- Restriction rules for external objects don't include organization-wide defaults or sharing mechanisms.

- External objects don't appear in Object Manager. To navigate to an external object, enter *External Data Sources* in the Quick Find box in Setup, then select **External Data Sources**. Select an external object from the list view on this page.

 **Note:** You can also find external objects in the Most Recently Used list in Setup.

Performance Considerations

Restriction rules were built to support sharing needs in a performant way. Your data volume and architecture are also factors in rule performance.

- To test a rule's performance impact, take the record criteria to your API client of choice and run the query. If it's fast for a given user, the rule is likely to run efficiently. For objects with large data volumes, add three to five percent overhead to the record filter's performance.
- If it isn't performant, isolate the field that is slowing performance. Work with Salesforce customer support to get the field indexed.

SEE ALSO:

[Knowledge Article: Improve Performance of SOQL Queries using a Custom Index](#)

Restriction Rule Example Scenarios

Refer to these sample restriction rules, which fulfill different access requirements.

To implement these examples, navigate to a supported object in the Object Manager and click **Restriction Rules**.

Allow Users to See Only Specified Record Type

This restriction rule allows the designated users to see only the records that have a specified record type.

Criteria	Click Path	Field	Operator	Type	Value
User Criteria	User > Role ID	[\$User].UserRoleId	Equals	ID	00Exxxxxxxxxxxx
Record Criteria	<i>Object > Object</i> Record Type ID > Name	[<i>Object</i>].RecordType.Name	Equals	String	Sample Record Type Name

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise, Performance, Unlimited, and Developer** Editions

Allow Users to See Only Records That They Own

This restriction rule allows users with the designated profile to see only the tasks that they own.

Criteria	Click Path	Field	Operator	Type	Value
User Criteria	User > Profile ID	[\$User].ProfileId	Equals	ID	00exxxxxxxxxxxx
Record Criteria	<i>Task > Assigned To ID (User)</i> User ID	[<i>Task</i>].Owner:User.Id	Equals	Current User	\$User.Id

Allow Users to See Only Records Owned by Same Role

This restriction rule allows active users to see only the events owned by users that have the same role.

Criteria	Click Path	Field	Operator	Type	Value
User Criteria	User > Active	[\$User].IsActive	Equals	Boolean	True
Record Criteria	<i>Event > Assigned To ID (User)</i> Role ID	[Event].Owner:User.UserRoleId	Equals	Current User	\$User.UserRoleId

Allow Users to See Only Records Owned by Same Profile

This restriction rule allows active users to see only the events owned by users that have the same profile.

Criteria	Click Path	Field	Operator	Type	Value
User Criteria	User > Active	[\$User].IsActive	Equals	Boolean	True
Record Criteria	<i>Event > Assigned To ID (User)</i> Profile ID	[Event].Owner:User.ProfileId	Equals	Current User	\$User.ProfileId

Allow Users to See Records Based on a Custom Field

This restriction rule allows high-volume users to see only the contracts where the user's department matches the contract's department. This rule uses a custom field, Department__c that must have the appropriate value set through Apex, Process Builder, workflows, or flows.

Criteria	Click Path	Field	Operator	Type	Value
User Criteria	User > User Type	[\$User].UserType	Equals	Picklist	High Volume Portal
Record Criteria	<i>Contract > Department</i>	[Contract].Department__c	Equals	Current User	\$User.Department

Allow Users to See an External Object's Records

This restriction rule allows active Salesforce users to see the records of an external object called Purchase Order. The rule uses a field called IsClosed on Purchase Order records in its record criteria.

 **Note:** Only external objects created using the Salesforce Connect: OData 2.0, OData 4.0, and Cross-Org adapters support restriction rules. Find out more in Restriction Rule Considerations.

Criteria	Click Path	Field	Operator	Type	Value
User Criteria	User > Department	[\$User].Department	Equals	String	Accounting
Record Criteria	<i>PurchaseOrder__X></i> IsClosed__c	[PurchaseOrder__x].IsClosed__c	Equals	String	false

Provide User Access With Multiple String or ID Values in Record Criteria

This restriction rule allows active users to see records whose Name__c field matches the rule's record criteria values. The record criteria contains strings separated by a comma. ID values are also supported. Double-quotes specify that the value inside the quotes isn't considered a delimiter.

This rule uses a custom object called Agent__c with a custom text field called Name__c.

Criteria	Click Path	Field	Operator	Type	Value
User Criteria	User > Active	[\$User].IsActive	Equals	Boolean	True
Record Criteria	<i>Agent__c</i> > Name__c	[<i>Agent__c</i>].Name__c	Equals	String	Tom, Anita, "Torres, Jia"

This restriction rule allows active users to see records owned by two different managers. In this example, the rule's record criteria contains ID's separated by a comma.

Criteria	Click Path	Field	Operator	Type	Value
User Criteria	User > Active	[\$User].IsActive	Equals	Boolean	True
Record Criteria	<i>Agent__cOwner ID (User)</i> Manager ID	[<i>Agent__c</i>].Owner:User:ManagerId	Equals	ID	001xx000003HNy7, 001xx000003HNut

SEE ALSO:

[Restriction Rule Considerations](#)

Scoping Rules

Scoping rules let you control the records that your users see based on criteria that you select. You can set up scoping rules for different users in your Salesforce org so that they can focus on the records that matter to them. Users can switch the set of records they're seeing as needed.

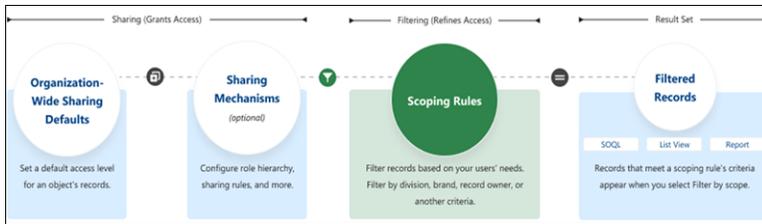
Scoping rules are available for custom objects and the account, case, contact, event, lead, opportunity, and task standard objects. Any partner, ISV, or customer can test scoping rules using a Developer Edition org. Scoping rules are turned on in Developer editions created after April 2022.

This table shows how scoping rules work with other Salesforce features.

Feature	Description
List Views	Applied in Lightning Experience if Filter by scope is selected
Reports	Applied in Lightning Experience if Filter by scope is selected
SOQL	Applied, unless a scope other than <i>scopingrule</i> is specified

EDITIONS

Available in: Lightning Experience in **Performance, Unlimited,** and **Developer** editions.



When Do I Use Scoping Rules?

Use scoping rules when you want to let users control the record set that they see. A scoping rule doesn't restrict users' access to other records that they sometimes need. Instead, scoping rules let your users focus on one set of records, then change their focus or search to find a record that's not in the scoped record set when they need to.

For example, you have users who support multiple agencies in your org. Each user is assigned to a specific agency. You can set up scoping rules so that they filter the records that your users see in list views and reports. Users don't need to spend time looking for the correct records, but they still have access to the other agencies' records if they need them.

You can also use scoping rules with Flow Builder to set scope according to a choice your user makes. For example, you have users who work on account records that belong to different divisions in your organization. You want to scope the account records that users see by division, giving your users an easy way to switch between different divisions' record sets. You can set up a flow that your users access using the Lightning Utility Bar to set the scope of records that the user sees in list views, reports, and other features.

How Do Scoping Rules Affect User Access?

Scoping rules are flexible. You can enable and disable them on a query-by-query basis. Plus, they don't restrict the access that your users have to records. Your users can still open and report on all the records that they can access according to your org's sharing settings.

How Do I Configure Scoping Rules?

Create and manage scoping rules by navigating to a supported object in the Object Manager. Or use the `RestrictionRule Tooling API` object or `RestrictionRule Metadata API` type. For information on restriction rules, see the [Restriction Rule Developer Guide](#).

When creating more than one scoping or restriction rule, configure the rules so that only one active rule applies to a given user. Salesforce doesn't validate that only one active rule applies for a given user. If you create two active rules, and both rules apply to a given user, only one of the active rules is observed.

After creating rules, you can use a change set or unlocked package to move scoping rules from one org to another.

[Create a Scoping Rule](#)

Determine which records your users see by default. When a scoping rule is applied to a user, the data that the user sees in list views and reports is filtered by the criteria you set.

[Scoping Rule Considerations](#)

Keep these considerations and limitations in mind while using scoping rules.

Scoping Rule Example Scenarios

Refer to these sample scoping rules, which fulfill different access requirements.

SEE ALSO:

[Metadata API Guide: RestrictionRule](#)

[Tooling API Guide: RestrictionRule](#)

[Salesforce Help: Flow Builder](#)

Create a Scoping Rule

Determine which records your users see by default. When a scoping rule is applied to a user, the data that the user sees in list views and reports is filtered by the criteria you set.

Scoping rules are available for custom objects, accounts, cases, contacts, events, tasks, leads, and opportunities.

Your edition affects how many active rules you can have.

- Create up to two active scoping rules per object in Developer editions.
- Create up to five active scoping rules per object in Performance and Unlimited editions.

1. In Object Manager, click the object name for your scoping rule.

2. In the sidebar, click **Scoping Rule**, and then click **New Rule**.

3. Enter the rule's name and modify the autogenerated full name if necessary. The full name is the name of the component used by the API.

4. To have the rule take effect upon saving, select **Is Active**.

5. Under User Criteria, select which users this scoping rule applies to.

- If the rule applies to a subset of users such as those in a given role, profile, or department, select **User Criteria**. Then, select the field to use as criteria.

Set the Type field as **Current User** when the rule applies to the currently logged-in user.

- If the rule applies to a subset of users with a custom permission, select **Permission Criteria**.

To filter records for users with the custom permission, set the Boolean value to **True**. To filter records for users who don't have the custom permission, set the Boolean value to **False**.

6. Under Record Criteria, select which records the specified users see by default. For the Field value, you can reference another object's field using dot notation.

To designate more than one value in the record criteria, you can specify a list of comma-separated strings or 15-character IDs in the Value field.

 **Tip:** To include a single value that contains a comma, surround the value with double quotes ("").

7. Save the rule.

EDITIONS

Available in: Lightning Experience in **Performance, Unlimited,** and **Developer** editions.

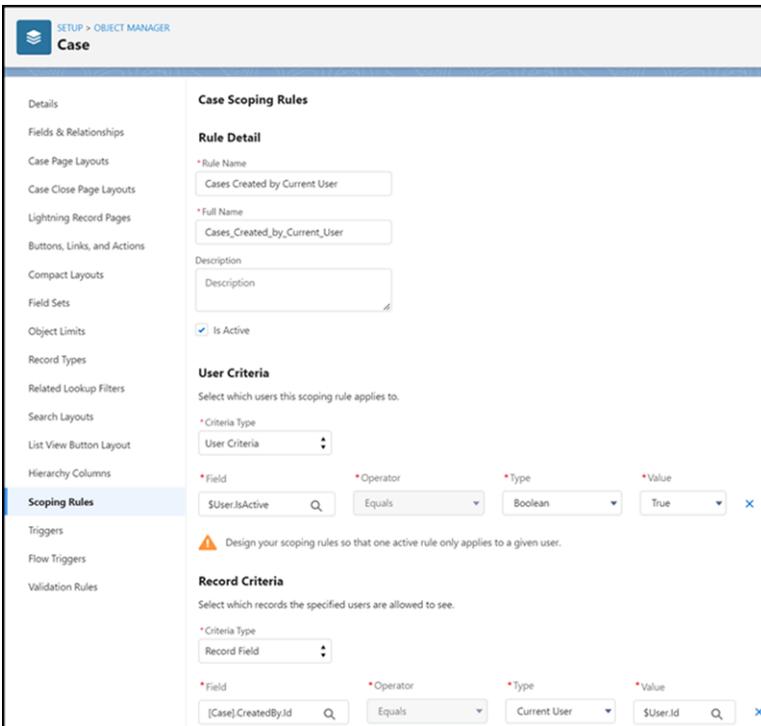
USER PERMISSIONS

To create and manage scoping rules:

- **Manage Sharing**

To view scoping rules:

- **View Setup & Configuration AND View Restriction and Scoping Rules**



SETUP > OBJECT MANAGER
Case

Details

Fields & Relationships

Case Page Layouts

Case Close Page Layouts

Lightning Record Pages

Buttons, Links, and Actions

Compact Layouts

Field Sets

Object Limits

Record Types

Related Lookup Filters

Search Layouts

List View Button Layout

Hierarchy Columns

Scoping Rules

Triggers

Flow Triggers

Validation Rules

Case Scoping Rules

Rule Detail

* Rule Name
Cases Created by Current User

* Full Name
Cases_Created_by_Current_User

Description
Description

Is Active

User Criteria

Select which users this scoping rule applies to.

* Criteria Type
User Criteria

* Field
\$User.IsActive

* Operator
Equals

* Type
Boolean

* Value
True

⚠ Design your scoping rules so that one active rule only applies to a given user.

Record Criteria

Select which records the specified users are allowed to see.

* Criteria Type
Record Field

* Field
[Case].CreatedBy.Id

* Operator
Equals

* Type
Current User

* Value
\$User.Id

 **Note:** Salesforce doesn't validate that only one active rule applies for a given user. If you create two active rules, and both rules apply to a given user, only one of the active rules is observed.

After you activate a scoping rule, users select the filter option **Filter by Scope** to update their list view or report filter and focus on a filtered set of records.

[Create a Flow That Applies a Scoping Rule](#)

You can create a scoping rule and then create a flow that users can run to update their user record. Users can filter records by scope to see only the records they need to focus on.

SEE ALSO:

[Enable Custom Permissions in Permission Sets](#)

Create a Flow That Applies a Scoping Rule

You can create a scoping rule and then create a flow that users can run to update their user record. Users can filter records by scope to see only the records they need to focus on.

This scoping rule scopes records according to their division.

1. [Create a scoping rule](#) that scopes the records by division, matching the record's division to the current user's division.
2. [Create a flow](#) in Flow Builder.
 - a. Use a Screen Flow.
 - b. Create a Choice resource for each division.
 - c. Use a Screen element to let users select a division.
 - d. Use an Update Records element to update the division on the current user's record.
3. Activate your flow.
4. [Distribute your flow](#) to users who need to run it.

 **Example:** Add a flow to a utility bar so users can run the flow. In App Manager, find the Lightning or Connected app where the flow needs to appear. Add the flow to a utility bar that users can click, causing a different scope to apply. In the flow detailed here, users click the utility bar to update the division on their user record. If a different scope applies, it's applied when the user runs the flow.

 **Tip:** Make sure that users who want to run your flow have the Run Flows permission.

After updating their division, users select the filter option **Filter by Scope** to update their list view or report filter and focus on a different set of records.

SEE ALSO:

[Salesforce Help: Flow Builder](#)

[Salesforce Help: Add a Flow to a Utility Bar](#)

Scoping Rule Considerations

Keep these considerations and limitations in mind while using scoping rules.

Creating Scoping Rules

Your edition affects how many active rules you can have.

- Create up to two active scoping rules per object in Developer editions.
- Create up to five active scoping rules per object in Performance and Unlimited editions.
- Create only one scoping or restriction rule per object per user. For a given object, only one scoping or restriction rule's user criteria field must evaluate to `true` for a given user.
- Creating a scoping rule for an object impacts only that object and doesn't affect child objects.
- When you reference the Owner field, you must specify the object type in your syntax. For example, the Owner field on an Event object can contain a user or a queue, but queues aren't supported in scoping rules. So it's necessary to specify Owner:User in the record criteria syntax when the criteria allows only users.

EDITIONS

Available in: Lightning Experience in **Performance, Unlimited,** and **Developer** editions.

USER PERMISSIONS

To create and manage scoping rules:

- Manage Sharing

To view scoping rules:

- View Setup & Configuration AND View Restriction and Scoping Rules

To open, edit, or create a flow in Flow Builder:

- Manage Flow

EDITIONS

Available in: Lightning Experience

Available in: **Performance** and **Unlimited** Editions

- You can reference another object's field using dot notation in the record criteria field. You can use only one "dot" (one lookup level from the target entity). For example, `Owner.UserRoleId`.
- In the rule's record criteria, you can't reference fields on the object's parent. For example, if you're creating a rule for the Task object, the record criteria can't reference a field on the parent Activity object.
- These data types are supported in the record and user criteria fields.
 - boolean
 - date (yyyy-MM-dd)
 - dateTime (yyyy-MM-dd HH:mm:ss)
 - double
 - int
 - reference
 - string
 - time
 - single picklist

 **Note:** Comma-separated ID or string values are supported in the Record Criteria field.

- Don't create rules on `Event.IsGroupEvent`, which indicates whether the event has invitees.
- Scoping rules on Open Activity or Activity History related lists aren't supported. Instead use the Activity Timeline or create a rule on the Task or Event object that uses fields available in the OpenActivity or ActivityHistory object.
- For list views and reports, you can apply the scope through Metadata API (using the `filterScope` field on the ListView type and the `scope` field on the Report type "scope").
- Unless you use SOQL, scoping rules support only the EQUALS operator. The AND and OR operators aren't supported.
- When using the SOQL operator in the record criteria, the SELECT statement, including nested SELECT statements, must include `USING SCOPE EVERYTHING`. `USING SCOPE EVERYTHING` is the only valid scope clause syntax for scoping rules.
- The SOQL operator doesn't support `$User` syntax except for `$User.Id`. Dynamic queries within the SOQL operator aren't supported, including on other user object fields.

 **Example:** Supported SOQL Syntax

```
SOQL(Id, SELECT Account.id FROM AccountAdvisors USING SCOPE EVERYTHING WHERE userid
= $User.Id)
```

Unsupported SOQL Syntax

```
SOQL(Id, SELECT Account.id FROM AccountAdvisors USING SCOPE EVERYTHING WHERE userid
= $User.Current_Advisor__c)
```

- Using the same object as the SOQL Query object and the Scoping Rule object isn't supported.
- The left operand in the SOQL type RecordCriteria must query a single ID (primary key) or reference (foreign key) field. See Comparison Operators for a list of valid operators that you can use in the field expression of a `WHERE` clause, which you use in a `SELECT` statement.

 **Example:** `"recordFilter": "SOQL(OwnerId, Select Id from User USING SCOPE Everything LIMIT 2) "`

The left operand is OwnerId in this example.

- If you include an ID in your record or user criteria field that is specific to your Salesforce org (such as a role, record type, or profile ID), you must modify the ID in the target org if it's different from the org where the scoping rule was originally created. Keep this consideration in mind when deploying rules between sandboxes or to a production org.

Modifying Scoping Rules

- Deleting custom fields that are referenced in scoping rules results in an error.
- To disable a scoping rule, first delete the list views and reports that have **Filter by scope** selected. After a scoping rule is disabled, the list views and reports aren't functional nor modifiable.
- The scoping rule user criteria field supports custom permissions. If you delete the custom permission, the scoping rules that use the custom permissions don't work.
- Scoping rules support custom picklist values in record and user criteria. If you delete a custom picklist value used in a scoping rule, the rule no longer works as intended.

Accounts, Contacts, and Person Accounts

- Scoping rules don't support IsPersonAccount fields on the account object. When setting a scoping rule, don't use IsPersonAccount fields such as PersonDepartment or PersonLeadSource in record criteria. Find a list of IsPersonAccount fields on the [Account](#) page.
- An error can result if you navigate to a person account detail page from a Contacts list view. To navigate to a person account detail page when there's a scoping rule on the account object, use an Accounts list view such as All Accounts.
- In related lists, all associated records that a user can access are visible, regardless of scope, except in the contact role related list. When a scoping rule is applied on the contact object, scope is applied to the [contact role](#) related list that appears on account, opportunity, case, and contract records. So it's possible that users, such as members of a sales team, can see a filtered set of contact roles without knowing that the list is filtered.
- When an org uses duplicate rules to prevent creating duplicate records, scoping rules limit the potential duplicates that are shown, even when **Bypass sharing rules** is turned on. Duplicate records are limited by the scope set in the scoping rule.

Performance Considerations

Scoping rules were built to support sharing needs in a performant way. Your data volume and architecture are factors in rule performance. Salesforce reserves the right to disable a scoping rule if a rule you create is inefficient or if your data model has so much data that scoping rules cause slowness when applied. To prevent throttling or deactivation, test the scoping rules that you plan to apply in a sandbox environment before enabling them in production.

- To test the performance impact of a rule that uses a SOQL operator, take the SOQL statement and run it in your API client of choice. If it's fast for a given user, the rule is likely to run efficiently.
- If a rule isn't performant, isolate the field that is slowing performance. Work with Salesforce customer support to find out if the field can be indexed.

SEE ALSO:

[Knowledge Article: Improve Performance of SOQL Queries using a Custom Index](#)

[SOQL and SOSL Reference: Comparison Operators](#)

Scoping Rule Example Scenarios

Refer to these sample scoping rules, which fulfill different access requirements.

To implement these examples, navigate to a supported object in the Object Manager and click **Scoping Rules**.

EDITIONS

Available in: Lightning Experience in **Performance, Unlimited,** and **Developer** editions.

Display a Branch Location's Tasks by Default

This scoping rule displays task records associated with a particular bank branch location by default. A custom field called Branch__c stores the bank's branch locations.

Criteria	Click Path	Field	Operator	Type	Value
User Criteria	User > Role ID	\$User.UserRoleId	Equals	ID	00Exxxxxxxxxxxxx
Record Criteria	<i>Task</i> > Branch__c	[<i>Task</i>].Branch__c	Equals	String	Bank Branch 1

Display a Department's Contacts by Default

This scoping rule displays contact records associated with a particular department by default for a user who works on them. The rule dynamically matches the contact owner's department with the current user's department.

Criteria	Click Path	Field	Operator	Type	Value
User Criteria	User > Role ID	\$User.UserRoleId	Equals	ID	00Exxxxxxxxxxxxx
Record Criteria	<i>Contact</i> > Department	[<i>Contact</i>].Department	Equals	Current User	\$User.Department

Display a Division's Tasks by Default

This scoping rule displays records associated with a particular division by default for a user.

Criteria	Click Path	Field	Operator	Type	Value
User Criteria	User > Profile	\$User.Profile	Equals	ID	00Exxxxxxxxxxxxx
Record Criteria	<i>Task</i> > <i>Assigned To ID (User)</i> Division	[<i>Task</i>].Owner:User:Division	Equals	Current User	\$User.Division

Scope Records Using Multiple String or ID Values in Record Criteria

This scoping rule allows active users to scope the records they see to records whose Name__c field matches the rule's record criteria value. The record criteria contains strings separated by a comma. ID values are also supported. Double-quotes specify that the value inside the quotes isn't considered a delimiter.

This rule uses a custom object called Agent__c with a text field called Name__c.

Criteria	Click Path	Field	Operator	Type	Value
User Criteria	User > Active	[\$User].IsActive	Equals	Boolean	True
Record Criteria	<i>Agent__c</i> > Name__c	[<i>Agent__c</i>].Name__c	Equals	String	Tom, Anita, "Torres, Jia"

This scoping rule allows active users to see records owned by two different managers. In this example, the rule's record criteria contains ID's separated by a comma.

Criteria	Click Path	Field	Operator	Type	Value
User Criteria	User > Active	[\$User].IsActive	Equals	Boolean	True
Record Criteria	<i>Agent__cOwner ID (User)</i> Manager ID	[<i>Agent__c</i>].Owner:User:ManagerId	Equals	ID	001xx000003HNy7, 001xx000003HNut

Import Data Into Salesforce

Salesforce offers several ways to import your data. You can import up to 50,000 records into Salesforce.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small windows, while the Data Import Wizard opens in a full browser with `dataimporter.app` at the end of the URL. From Setup, enter *Data Import Wizard* in the **Quick Find** box, then select **Data Import Wizard**. The options you see depend on your permissions.

You can import data from ACT!, Outlook, and any program that can save data in comma-delimited text format (.csv), such as Excel or GoldMine.

Note: If commas aren't appropriate for your locale, use a tab or other delimiter. Specify your delimiter in Data Loader Settings (**Settings | Settings**).

The number of records you can import depends on your permissions and the type of data that you import. You can import as many records as allowed, as long as you don't exceed the overall data storage limits for your Salesforce org.

For information on field accessibility and how to import field value types, see [Notes on Importing Data](#) on page 684.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Your edition determines the types of objects you can import.

Online Salesforce Help

Other Resources

Plan Your Data Import

- [Choosing a Method for Importing Data](#)

- Video: [Data Import: Choosing the Right Tool](#)
- Developer Guide: [Data Loader Guide: When to Use Data Loader](#)
- Developer Guide: [Bulk API 2.0](#)
- Trailhead: [Lightning Platform API Basics](#) [Use Bulk API](#)

Plan Your Data Import	
	<ul style="list-style-type: none"> • Salesforce Developers Blog: Slim Down with the New Bulk API v2 • Developer Guide: Bulk API Developer Guide • Salesforce Developers Blog: How to Load Data into Salesforce? Let Me Count the Ways
<ul style="list-style-type: none"> • Data Loader • Perform Mass Updates • Running in Batch Mode • Mass Transfer Records 	<ul style="list-style-type: none"> • Video: ▶ Series: Managing Data Using the Data Loader • Developer Guide: Data Loader Guide: When to Use Data Loader
<ul style="list-style-type: none"> • Data Import Wizard • How do I use the Data Import Wizard to update records that match specified Salesforce IDs? 	<ul style="list-style-type: none"> • Video: ▶ Using the Data Import Wizard • Salesforce Developers Blog: Data Import Wizard—Comparison with Existing Wizards • Trailhead: 🗺️ Import and Export with Data Management Tools Use the Data Import Wizard
<ul style="list-style-type: none"> • Running in Batch Mode • Command-Line Quick Start 	<ul style="list-style-type: none"> • Developer Guide: Salesforce CLI Command Reference
<ul style="list-style-type: none"> • Run Batch File With Windows Command-Line Interface 	
<ul style="list-style-type: none"> • Import Limits 	<ul style="list-style-type: none"> • Salesforce Developer Limits and Allocations Quick Reference: Bulk API Allocations

Prepare Your Data for Import	
<ul style="list-style-type: none"> • Prepare Your Data for Import 	<ul style="list-style-type: none"> • Developer Guide: Bulk API 2.0 Prepare CSV Files • Video: ▶ How To Import Data into Salesforce Series Data Import: Owner IDs and Parent IDs • Video: ▶ Improve Your Data Quality Enable the User Experience with Data • Video Series: ▶ Data Management Strategy: Get The Most Out Of Your Data

Import Your Data	
<p>Import Data Into Salesforce</p>	<ul style="list-style-type: none"> • Trailhead: 🗺️ Data Management Import Data • Trailmix: 🗺️ Getting Started - Import Your Data

Import Your Data	
<ul style="list-style-type: none"> • Import Data Into Salesforce • Importing Records • Import Person Accounts • Add Person Accounts with the Data Import Wizard 	<ul style="list-style-type: none"> • Video: How To Import Data into Salesforce Series • Video: Improve Your Data Quality Enable the User Experience with Data • Video: Moving From Spreadsheets to the Cloud • Video: Loading Data

Use Best Practices for Loading Data	
<ul style="list-style-type: none"> • Data Quality 	<ul style="list-style-type: none"> • Trailhead: Data Quality • Video: How To Import Data into Salesforce Series • Video: Data Import: Best Practices for Importing Data
	<ul style="list-style-type: none"> • Developer Guide: Best Practices with Any Data Loader • Developer Guide: Best Practices for Deployments with Large Data Volumes • Developer Guide: General Guidelines for Data Loads Volumes • Video (2): Data Import: Clean Up Your Import File • Video (3): Data Import: Clean and Prepare Your Data Using Excel • Developer Article: Salesforce Bulk API - Maximizing Parallelism and Throughput Performance When Integrating or Loading Large Data Volumes • Trailhead: Large Data Volumes Load Your Data

Monitor Your Data Import	
<ul style="list-style-type: none"> • General Importing Questions 	<ul style="list-style-type: none"> • Developer Guide: Best Practices for Deployments with Large Data Volumes: Large Data Volumes Case Studies
<ul style="list-style-type: none"> • Manage Duplicate Records 	<ul style="list-style-type: none"> • Trailhead: Duplicate Management

SEE ALSO:

[Data Import Wizard](#)

[Choosing a Method for Importing Data](#)

[Undoing an Import](#)

[What permissions do I need to import records?](#)

Importing Records

The number of records you can import depends on your permissions and the type of data you're importing. You can import as many records as allowed, as long as you don't exceed the overall data storage limits for your org.

Which records can be imported?

Type of record	Import record limit	Users permissions needed	Learn more
Business accounts and contacts owned by you	50,000 at a time via the Data Import Wizard	Import Personal Contacts	What Is Imported for Business Accounts and Contacts?
Business accounts and contacts owned by other users	50,000 at a time	Modify All Data	What Is Imported for Business Accounts and Contacts?
Person accounts owned by you	50,000 at a time	Create on accounts AND Edit on accounts AND Import Personal Contacts	What Is Imported for Person Accounts?
Person accounts owned by other users	50,000 at a time	Create on accounts AND Edit on accounts and contacts AND Modify All Data	What Is Imported for Person Accounts?
Leads	50,000 at a time	Import Leads	What Is Imported for Leads?
Campaign members	50,000 at a time	Depends on what's being imported: <ul style="list-style-type: none"> • Campaign member statuses • Existing contacts • Existing leads • Existing person accounts • New contacts • New leads 	What's Imported for Campaign Members? Who can import campaign members?

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer Editions

Which records can be imported?

Type of record	Import record limit	Users permissions needed	Learn more
Custom objects	50,000 at a time	Import Custom Objects AND Create on the custom object AND Edit on the custom object	What Is Imported for Custom Objects?
Solutions	50,000 at a time	Import Solutions	What Is Imported for Solutions?
Assets	You can't import these records via the Data Import Wizard.		
Cases			
Campaigns			
Contracts			
Documents			
Opportunities			
Products			

For information on field accessibility and how different field type values are imported, see [Notes on Importing Data](#) on page 684. Relationship group members can't be imported.

Choosing a Method for Importing Data

Learn about your options for importing data into Salesforce.

Tool	Editions supported	Number of records you can import or export	Import	Export	Internal or external to Salesforce	Additional information
Basic Data Import	Enterprise, Performance, Unlimited	Up to 50,000	Yes	No	Internal	An in-browser tool that provides a simplified approach for users who only need to import contacts and leads. For details, see Contact and Lead Imports in Sales Cloud.
Data Import Wizard	All, except Personal and Database.com Editions	Up to 50,000	Yes	No	Internal	An in-browser wizard that imports your org's accounts, contacts, leads, solutions, campaign members, and custom objects. Read more.

Tool	Editions supported	Number of records you can import or export	Import	Export	Internal or external to Salesforce	Additional information
Data Loader	Enterprise, Unlimited, Performance, Developer, and Database.com Editions	Between 5,000 and 5 million	Yes	Yes	External	Data Loader is an application for the bulk import or export of data. Use it to insert, update, delete, or export Salesforce records. Read more.
dataloader.io	All	Varies by dataloader.io plan	Yes	Yes	External	Dataloader.io is a cloud-based data import tool powered by Mulesoft. For product details, see the pricing overview .

SEE ALSO:

[Data Import Wizard](#)[Import Data Into Salesforce](#)

What Is Imported for Business Accounts and Contacts?

The Data Import Wizard allows you to match records in multiple ways to prevent duplicates. You can match contacts by Salesforce ID, name, email, or external ID. You can match business accounts by Salesforce ID, external ID, or by name and site. Matching by Salesforce ID is inclusive of both contacts and business accounts. If you match one by Salesforce ID, the other is also matched by Salesforce ID.

Matching by Name and Site

If you are matching contacts by name and business accounts by name and site (which are the recommended options), the Data Import Wizard creates a business account for each unique business account name and site in the import file. It also creates a separate contact for each contact name listed in the file. The contacts are then associated with the appropriate business accounts.

If the business account or contact exists in the system, and you have read/write access to the record, the wizard adds your import data to the existing data in Salesforce.

Matching by Salesforce ID

You can also choose to match contacts and business accounts by Salesforce ID. With this option, the Salesforce ID is the criteria for de-duplication. That is, if you are matching by ID and a record in your source file has the same ID as a record in Salesforce, that record is updated in Salesforce. Record IDs are case-sensitive and must match exactly.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All** Editions, except **Database.com**

Org import not available in: **Personal** Edition, **Database.com**

Matching by External ID

An external ID is a custom field that has the External ID attribute, meaning that it contains unique record identifiers from a system outside of Salesforce. When you select this option, the Data Import Wizard detects existing records in Salesforce with external IDs that match those values in the import file.

- This operation isn't case-sensitive. For example, "ABC" is matched with "abc". However, if the external ID field also has the case-sensitive Unique attribute, matching by external ID does not consider uppercase and lowercase letters identical.
- External IDs can be of type text, number, email, or auto-number. If the external ID type is auto-number, it isn't available for matching, but you can use it to look up the parent record if it contains the external ID.
- Standardize External ID values before performing the import to prevent unintended matches.
- Multiple records with the same External ID within a file aren't uploaded.
- Multiple external ID fields can find matching records in Salesforce when you use the Data Import Wizard.
- Only unique External ID fields are available to match by.

Overwriting Existing Account Values

The wizard never overwrites your existing business account fields unless you select **Overwrite existing account values**. This option lets you insert or update existing business account fields with new data. However, you cannot use this option to update existing field data with blank values. If you do not select this option, the wizard updates the empty business account fields, but does not touch fields with data.

If you do not have read/write access to an existing business account or contact, the wizards create a new business account or contact owned by you. In addition, the wizards create new business accounts and contacts based on specific fields in your import file.

In Professional, Enterprise, Unlimited, Performance, and Developer Edition orgs, the import wizards can also import new business account and contact notes. The wizards do not import notes that are exact duplicates of existing contact or business account notes.

To import account or contact notes, make the owner field in the imported file the Salesforce ID.

SEE ALSO:

[Data Import Wizard](#)

[Choosing a Method for Importing Data](#)

[Import Data Into Salesforce](#)

What Is Imported for Person Accounts?

The Data Import Wizard prevents creating duplicate person accounts by matching records according to one of the following fields: Account Name, Salesforce ID, Email, or an external ID field. In your import file, include a column for the field that you're using for record matching.

 **Note:** Your administrator could have renamed "person account" to another term. If so, the Data Import Wizard refers to the new name.

Matching by Name

When you select this option, the Data Import Wizard detects existing records in Salesforce that have the same name. This type of matching is case-sensitive. If necessary, scan and standardize your record names before performing the import to prevent unintended matches.

Matching by Salesforce ID

A Salesforce ID is a system-generated, case-sensitive string of 15 or 18 letters and numbers that uniquely identifies each Salesforce record. When you select this option, the Data Import Wizard detects existing records in Salesforce that have the same Salesforce ID. You can obtain Salesforce IDs by running reports that include the ID field of the record.

Matching by Email

This option matches records in your import file with existing records in Salesforce according to the exact value in the Email field.

Matching by External ID

An external ID is a custom field that has the External ID attribute, meaning that it contains unique record identifiers from a system outside of Salesforce. When you select this option, the Data Import Wizard detects existing records in Salesforce with external IDs that match those values in the import file.

- This operation isn't case-sensitive. For example, "ABC" is matched with "abc". However, if the external ID field also has the case-sensitive Unique attribute, matching by external ID does not consider uppercase and lowercase letters identical.
- External IDs can be of type text, number, email, or auto-number. If the external ID type is auto-number, it isn't available for matching, but you can use it to look up the parent record if it contains the external ID.
- Standardize External ID values before performing the import to prevent unintended matches.
- Multiple records with the same External ID within a file aren't uploaded.
- Multiple external ID fields can find matching records in Salesforce when you use the Data Import Wizard.
- Only unique External ID fields are available to match by.

Ignoring or Updating Matching Records

When the Data Import Wizard detects existing records in Salesforce that match according to your chosen field, you can choose one of these actions.

- **Add new records**—If records in your file are new and don't match existing records, insert them into Salesforce. Ignore records in your file that match existing records, and do nothing to the existing records.
- **Update existing records**—If records in your file match existing records, update the existing records. Ignore records in your file that don't match existing records, and don't insert them as new records.

EDITIONS

Data Import Wizard available in both Salesforce Classic and Lightning Experience

Data Import Wizard available in **All** Editions except Database.com

Person accounts available in: both Salesforce Classic and Lightning Experience

Person accounts available in **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

- **Add new and update existing records**—If records in your file are new and don't match existing records, insert them into Salesforce. If records in your file match existing records, update the existing records.

What Is Imported for Leads?

You can import data into standard lead fields and custom lead fields, even if a field is hidden or read only in your page layout or field-level security settings for leads.

Importing Leads with Matching Types

You can choose whether to match leads in your import file with existing leads in Salesforce. Leads can be matched according to the following types: Salesforce ID, name, email, or external ID. Choosing a matching type sets the criteria for avoiding duplicate leads. For example, if you're matching by email and a lead in your source file has the same email as a lead in Salesforce, that lead is updated in Salesforce. If you aren't matching by email and a lead in your source file has the same email as a lead in Salesforce, a lead is created.

Importing Leads Without Matching Types

If you choose a matching type of "None" in the Data Import Wizard, for each lead in your import file, the Data Import Wizard creates a lead in Salesforce. You can merge leads after they are imported.

Matching by Name

When you select this option, the Data Import Wizard detects existing records in Salesforce that have the same name. This type of matching is case-sensitive. If necessary, scan and standardize your record names before performing the import to prevent unintended matches.

Matching by Email

This option matches records in your import file with existing records in Salesforce according to the exact value in the Email field.

Matching by Salesforce ID

A Salesforce ID is a system-generated, case-sensitive string of 15 or 18 letters and numbers that uniquely identifies each Salesforce record. When you select this option, the Data Import Wizard detects existing records in Salesforce that have the same Salesforce ID. You can obtain Salesforce IDs by running reports that include the ID field of the record.

Matching by External ID

An external ID is a custom field that has the External ID attribute, meaning that it contains unique record identifiers from a system outside of Salesforce. When you select this option, the Data Import Wizard detects existing records in Salesforce with external IDs that match those values in the import file.

- This operation isn't case-sensitive. For example, "ABC" is matched with "abc". However, if the external ID field also has the case-sensitive Unique attribute, matching by external ID does not consider uppercase and lowercase letters identical.
- External IDs can be of type text, number, email, or auto-number. If the external ID type is auto-number, it isn't available for matching, but you can use it to look up the parent record if it contains the external ID.
- Standardize External ID values before performing the import to prevent unintended matches.
- Multiple records with the same External ID within a file aren't uploaded.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer Editions

- Multiple external ID fields can find matching records in Salesforce when you use the Data Import Wizard.
- Only unique External ID fields are available to match by.

SEE ALSO:

[Data Import Wizard](#)

[Choosing a Method for Importing Data](#)

What's Imported for Campaign Members?

You can use the Data Import Wizard to update the statuses of campaign members.

You can also import campaign members. For each contact, lead, or person account in your import file, the Data Import Wizard:

- Imports the record
- Associates the record with the specified campaign, making the contact, lead, or person account a campaign member
- Inserts a Member Status value for the campaign member

If your import file has duplicate records, the Data Import Wizard doesn't merge them. If an imported record matches an existing record, the Data Import Wizard doesn't merge the duplicate data into one record.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Matching by External ID

An external ID is a custom field that has the External ID attribute, meaning that it contains unique record identifiers from a system outside of Salesforce. When you select this option, the Data Import Wizard detects existing records in Salesforce with external IDs that match those values in the import file.

- This operation isn't case-sensitive. For example, "ABC" is matched with "abc". However, if the external ID field also has the case-sensitive Unique attribute, matching by external ID does not consider uppercase and lowercase letters identical.
- External IDs can be of type text, number, email, or auto-number. If the external ID type is auto-number, it isn't available for matching, but you can use it to look up the parent record if it contains the external ID.
- Standardize External ID values before performing the import to prevent unintended matches.
- Multiple records with the same External ID within a file aren't uploaded.
- Multiple external ID fields can find matching records in Salesforce when you use the Data Import Wizard.
- Only unique External ID fields are available to match by.

SEE ALSO:

[Data Import Wizard](#)

What Is Imported for Custom Objects?

The Data Import Wizard prevents creating duplicate records by matching records according to one of the following fields: custom object name, Salesforce ID, or external ID. In your import file, include a column for the field that you are using for record matching.

Matching by Name

When you select this option, the Data Import Wizard detects existing records in Salesforce that have the same name. This type of matching is case-sensitive. If necessary, scan and standardize your record names before performing the import to prevent unintended matches.

Matching by Salesforce ID

A Salesforce ID is a system-generated, case-sensitive string of 15 or 18 letters and numbers that uniquely identifies each Salesforce record. When you select this option, the Data Import Wizard detects existing records in Salesforce that have the same Salesforce ID. You can obtain Salesforce IDs by running reports that include the ID field of the record.

Matching by External ID

An external ID is a custom field that has the External ID attribute, meaning that it contains unique record identifiers from a system outside of Salesforce. When you select this option, the Data Import Wizard detects existing records in Salesforce with external IDs that match those values in the import file.

- This operation isn't case-sensitive. For example, "ABC" is matched with "abc". However, if the external ID field also has the case-sensitive Unique attribute, matching by external ID does not consider uppercase and lowercase letters identical.
- External IDs can be of type text, number, email, or auto-number. If the external ID type is auto-number, it isn't available for matching, but you can use it to look up the parent record if it contains the external ID.
- Standardize External ID values before performing the import to prevent unintended matches.
- Multiple records with the same External ID within a file aren't uploaded.
- Multiple external ID fields can find matching records in Salesforce when you use the Data Import Wizard.
- Only unique External ID fields are available to match by.

SEE ALSO:

[Data Import Wizard](#)

[Choosing a Method for Importing Data](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Custom object import available in: **Contact Manager, Essentials, Group, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To import custom object data via the Data Import Wizard:

- Import Custom Objects AND Create on the custom object

What Is Imported for Solutions?

The Data Import Wizard prevents creating duplicate records by matching records according to one of the following fields: solution title, Salesforce ID, or external ID. In your import file, include a column for the field that you are using for record matching.

Matching by Solution Title

When you select this option, the import wizard detects existing solutions in Salesforce that have the same title. This type of matching isn't case-sensitive. For example, titles that begin with a capital letter are matched with the same title that begins with a lowercase letter. If necessary, scan and standardize your solution titles before performing the import to prevent unintended matches.

Matching by Salesforce ID

A Salesforce ID is a system-generated, case-sensitive string of 15 or 18 letters and numbers that uniquely identifies each Salesforce record. When you select this option, the Data Import Wizard detects existing records in Salesforce that have the same Salesforce ID. You can obtain Salesforce IDs by running reports that include the ID field of the record.

Matching by External ID

An external ID is a custom field that has the External ID attribute, meaning that it contains unique record identifiers from a system outside of Salesforce. When you select this option, the Data Import Wizard detects existing records in Salesforce with external IDs that match those values in the import file.

- This operation isn't case-sensitive. For example, "ABC" is matched with "abc". However, if the external ID field also has the case-sensitive Unique attribute, matching by external ID does not consider uppercase and lowercase letters identical.
- External IDs can be of type text, number, email, or auto-number. If the external ID type is auto-number, it isn't available for matching, but you can use it to look up the parent record if it contains the external ID.
- Standardize External ID values before performing the import to prevent unintended matches.
- Multiple records with the same External ID within a file aren't uploaded.
- Multiple external ID fields can find matching records in Salesforce when you use the Data Import Wizard.
- Only unique External ID fields are available to match by.

SEE ALSO:

[Data Import Wizard](#)

[Choosing a Method for Importing Data](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To import solutions:

- Import Solutions

Notes on Importing Data

Review these notes when importing data into Salesforce.

Field Accessibility

You can import values into a field only if you have read and edit access. User permissions, page layout assignments, and field-level security settings determine field access.

Field-level security is available in Professional, Enterprise, Unlimited, Performance, and Developer Editions.

New Values for Picklists and Multi-Select Picklists

If you import a picklist value that doesn't match an existing picklist value:

- For an unrestricted picklist, the Data Import Wizard uses the value that's in the import file.
- For a restricted picklist, the Data Import Wizard uses the picklist's default value.

Multi-Select Picklists

To import multiple values into a multi-select picklist, separate the values by a semicolon in your import file.

You can import up to 100 values at a time in a multi-select picklist field. If you have more than 100 values in your import file for any one record, the import wizard leaves the field blank in that record.

Checkboxes

To import data into a checkbox field, use 1 for checked values and 0 for unchecked values.

Default Values

For picklist, multi-select picklist, and checkbox fields, if you do not map the field in the import wizard, the default value for the field, if any, is automatically inserted into the new or updated record.

Date/Time Fields

Ensure that the format of any date/time fields you are importing matches how they display in Salesforce per your locale setting.

Formula Fields

Formula fields cannot accept imported data because they are read only.

Field Validation Rules

Salesforce runs validation rules on records before they are imported. Records that fail validation aren't imported. Consider deactivating the appropriate validation rules before running an import if they affect the records you are importing.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Your edition determines the types of objects you can import.

Geolocation Custom Fields

To import a geolocation custom field using the Data Import Wizard, supply two values: a latitude and a longitude. Import both values in one field, separated by a semicolon. If you enter only one value, it is imported as the latitude, and the longitude is interpreted as 0. If you supply more than two values, the import fails for the entire row.

Currency Fields

If you have currency data in your CSV file, format your values for your locale. For example, if you're in the U.S. locale, use periods for decimals and commas for thousand markers. Using the incorrect currency format could change your imported values.

SEE ALSO:

[Data Import Wizard](#)

[Choosing a Method for Importing Data](#)

[Import Data Into Salesforce](#)

Rules for Importing Multiple Currencies

If your organization has set up the ability to use multiple currencies, you can import amounts in different currencies.

Organization Import

When importing accounts, contacts, custom objects, leads, or solutions for your organization, you can specify the currency type for amount fields using the `Currency ISO Code` column in your import file.

Entering currency codes	Enter a currency code in the <code>Currency ISO Code</code> column in your import file. Currency codes are three letter codes that follow an international standard. For example, USD is the currency code for U.S. dollars. From Setup, enter <i>Manage Currencies</i> in the <code>Quick Find</code> box, then select Manage Currencies to see a list of valid codes for your organization.
Updating the currency code	When updating the currency code but not the currency amount for accounts and contacts, the amount isn't converted to the corresponding number in the new currency.
Entering inactive currencies	If you enter an inactive currency in your import file, your personal currency is used instead. However, amounts aren't modified. For example, if your file has AUD 100 for 100 Australian dollars but AUD is an inactive currency for your organization, it's imported as USD 100, assuming your personal currency is U.S. dollars.
Omitting the <code>Currency ISO Code</code> column	When creating records via importing, if you don't use the <code>Currency ISO Code</code> column or fail to map it, your personal currency is used. For example, if your file has 100 and your personal currency is U.S. dollars (currency code = USD), it's imported as USD 100.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

When updating existing records via importing, if you don't use the `Currency ISO Code` column or fail to map it, any amounts are interpreted as having the currency of the record. For example, if your file has 100 for a record that has a currency of EUR (the currency code for euros), this amount is interpreted as EUR 100.

SEE ALSO:

[Data Import Wizard](#)

Create Export Files for Import Wizards

Before you can import data into Salesforce, use your existing software to create a data export file.

An export file contains all the information you want to import.

Your export file can contain a mixture of new records and updates to existing records. You'll choose how records are matched to avoid duplication. For example, you can choose to match accounts and contacts by name or by email address. If you choose to match by email address, then the contact already in Salesforce will be updated if a record in your imported data has the same email address. However, if records have the same name but different email addresses, the records will remain separate.

1. Use your existing software to create a data export file.
 - [Export Contact Data from ACT!](#)
 - [Exporting from LinkedIn®](#)
 - [Export from Outlook](#)
 - [Export from Other Data Sources](#)
 - [Export from Salesforce](#)
2. Review data you will import to ensure that it is more up-to-date than what is already in Salesforce. Your Salesforce data will be replaced with data from your import file, even if it is out of date.
3. Compare your data fields with the Salesforce fields you can import into, and verify that your data will be mapped into the appropriate Salesforce fields. See [Prepare Your Data for Import](#) on page 689.
4. If you are the administrator and are importing for multiple users, combine export data from multiple sources into a single comma delimited text file (.csv) using Excel.

When importing records from multiple users, your export file must include a `Record Owner` field for all new records which must contain the full usernames or first and last names of existing, active users. Existing record owners will not be changed; new records will be assigned to the user listed in the `Record Owner` field. For example, records that should be owned by Joe Smith in your organization must have that user's username ("jsmith@acme.com") or first and last names (for example, "Joe Smith", or "Smith Joe" for Asian locales). For lead imports, you can also specify the name of a lead queue.

When importing leads, you can alternatively use a lead assignment rule to specify the owners of the imported data, instead of using a `Record Owner` field.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer Editions

Export Contact Data from ACT!

ACT! allows you to export contact data in a text-delimited format which can then be imported.

To export contact data from ACT! (versions 4.0 or 2000):

1. Launch ACT! and open your database.
2. Select **File > Data Exchange > Export...**
3. Select the file type **Text-Delimited**.
4. Choose a file name and location for the exported data and click **Next**.
5. Select **Contact records only**.
6. Click the **Options...** button.
7. Select **Comma** for the field separator character. If commas aren't appropriate for your locale, use a tab or other delimiter. Specify your delimiter in Data Loader Settings (**Settings | Settings**).
8. Select **Yes, export field names** and click **OK**.
9. Click **Next**.
10. Select **All Records** and then click **Next**.
11. Leave the export field order list alone, and click **Finish**.

SEE ALSO:

[Default Field Mapping for ACT!](#)

[Create Export Files for Import Wizards](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions** except **Database.com**

Exporting from LinkedIn®

You can export contact data from LinkedIn in a text-delimited format, which you can then import.

- Open www.linkedin.com/addressBookExport and follow the steps on the page using the **Microsoft Outlook (.CSV file)** option.

Export from Outlook

Export data directly from Microsoft® Outlook® in a CSV (comma-separated values) format. Then import that data into Salesforce.

1. In Outlook, navigate to the export feature.
2. Choose **Comma Separated Values (Windows)** and click **Next**. If commas aren't appropriate for your locale, use a tab or other delimiter. Specify your delimiter in Data Loader Settings (**Settings | Settings**).
3. Select the folder containing the contacts you want to export, and click **Next**.
4. Choose a file name for the exported data and click **Next**.
5. Click **Finish**.

SEE ALSO:

[Default Field Mapping for Outlook](#)

[Create Export Files for Import Wizards](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **All Editions** except **Database.com**

Export from Other Data Sources

You can import data into the system from any other application that can create a CSV (comma-separated values) file.

1. Save your data source as a CSV file. If commas aren't appropriate for your locale, use a tab or other delimiter. Specify your delimiter in Data Loader Settings (**Settings** | **Settings**).
2. Ensure your file includes only one name per field. The system cannot accept more than one name per field.
3. Ensure your file separates names and titles into two fields. The system cannot accept fields containing both names and titles.
4. Ensure your file includes only one phone number per field.

SEE ALSO:

[Field Mapping for Other Data Sources and Organization Import](#)

[Create Export Files for Import Wizards](#)

Export from Salesforce

You can export account, campaign member, contact, custom object, lead, or solution reports from Salesforce to create an import file.

Include the `Account ID`, `Campaign Member ID`, `Contact ID`, `Custom Object ID`, `Lead ID`, or `Solution ID` value for each respective record in your report. These ID fields are unique Salesforce identifiers and are used to accurately match your data with existing Salesforce records.

 **Note:** Remember that Salesforce record IDs are case-sensitive. Don't manually change Salesforce IDs in your import file.

To create an import file with these ID fields, first export the data from Salesforce.

1. Run an account, campaign member, contact, custom object, lead, or solution report in Salesforce. Include the respective ID field and any other fields that are required for the import.
2. Export the report to Excel.

SEE ALSO:

[Create Export Files for Import Wizards](#)

[Videos: Data Import How-To Series](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Prepare Your Data for Import

After exporting your data from Salesforce or your existing application, prepare your data before importing it.

 **Note:** If your data has information in fields that do not match any standard fields, your admin can create custom fields for that data before import.

Preparing Contacts

Use Excel® to label the columns in your import file as specified in [Field Mapping for Other Data Sources and Organization Import](#) on page 695.

Preparing Person Accounts

When importing person accounts, use the field labels in Salesforce as the column labels in your import file.

Preparing Org Business Accounts and Contacts

When importing business accounts and contacts for your org, you must use Excel® to label the columns in your import file as specified in [Field Mapping for Other Data Sources and Organization Import](#) on page 695.

Preparing Org Leads

When importing general leads or leads for campaigns, use the import file labels specified in [Field Mapping for Importing Leads](#) on page 700.

Preparing Custom Objects

When importing a custom object, use the field labels shown on the custom object detail page in Salesforce as the column labels in your import file.

Preparing Campaign Members

When importing campaign members, use the field labels in Salesforce as the column labels in your import file.

Preparing Solutions

When importing solutions, use the field labels in Salesforce as the column labels in your import file.

You can enter HTML into the solutions you plan to import into Salesforce. However, unless your org has enabled HTML solutions, HTML tags will display in the solutions after they are imported.

For security purposes, Salesforce automatically filters all HTML solutions for potentially malicious HTML. If potentially malicious HTML is detected in an HTML solution, the potentially malicious HTML is either removed or transformed into text for users who view the HTML solution. Users can't notice when potentially malicious HTML is removed from an HTML solution.

You can import solutions written in HTML format into Salesforce. However, for security purposes, only the HTML tags listed below are allowed. The content of any HTML tags not listed below is removed when saved in HTML solutions. Furthermore, the content of all

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer Editions

<script> and <iframe> tags, as well as all JavaScript, is removed when saved in HTML solutions. Cascading Style Sheets (CSS) are not supported in HTML solutions.

The following HTML tags are allowed in HTML solutions imported into Salesforce:

| | | |
|--------------|--------|----------|
| <a> | <dt> | <q> |
| <abbr> | | <samp> |
| <acronym> | | <small> |
| <address> | <h1> | |
| | <h2> | <strike> |
| <bdo> | <h3> | |
| <big> | <h4> | <sub> |
| <blockquote> | <h5> | <sup> |
|
 | <h6> | <table> |
| <caption> | <hr> | <tbody> |
| <cite> | <i> | <td> |
| <code> | | <tfoot> |
| <col> | <ins> | <th> |
| <colgroup> | <kbd> | <thead> |
| <dd> | | <tr> |
| | | <tt> |
| <dfn> | <p> | |
| <div> | <pre> | <var> |
| <dl> | | |

Within the above tags, you can include the following attributes:

| | | |
|------------|---------|--------|
| alt | face | size |
| background | height | src |
| border | href | style |
| class | name | target |
| colspan | rowspan | width |

The above attributes, which can include a URL, are limited to URLs that begin with the following:

- http:

- `https:`
- `file:`
- `ftp:`
- `mailto:`
- `#`
- `/` for relative links

SEE ALSO:

[Default Field Mapping for ACT!](#)

[Default Field Mapping for Outlook](#)

[Create Export Files for Import Wizards](#)

Default Field Mapping for ACT!

ACT! fields map to Salesforce account and contact import fields during an individual data import.

If an ACT! record contains more than one contact for the same company, the import wizard creates multiple contacts for one account.

| ACT! Field | Import Field |
|------------------|--|
| Address 1 | Contact: Mailing Address and
Account: Billing Address |
| Address 2 | Contact: Mailing Address and
Account: Billing Address |
| Address 3 | Contact: Mailing Address and
Account: Billing Address |
| Alt Phone | Contact: Other Phone |
| Alt Phone Ext. | Contact: Other Phone Ext. |
| Assistant | Contact: Assistant's Name |
| Asst. Phone | Contact: Asst. Phone |
| Asst. Phone Ext. | Contact: Asst. Phone Ext. |
| City | Contact: Mailing City and
Account: Billing City |
| Company | Account: Name |
| Contact | Contact: Full Name |
| Country | Contact: Mailing Country and
Account: Billing Country |

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **All Editions** except **Database.com**

| ACT! Field | Import Field |
|--|--|
| Department | Contact: Department |
| E-mail Login | Contact: Email |
| (The import wizard verifies this is a valid email address in the form:
jsmith@acme.com) | |
| Fax | Contact: Fax and
Account: Fax |
| Fax Ext. | Contact: Business Fax Ext. |
| First Name | Contact: First Name |
| Home Address 1 | Contact: Other Address 1 |
| Home Address 2 | Contact: Other Address 2 |
| Home Address 3 | Contact: Other Address 3 |
| Home City | Contact: Other City |
| Home Country | Contact: Other Country |
| Home Phone | Contact: Home Phone |
| Home State | Contact: Other State |
| Home Zip | Contact: Other Postal Code |
| ID/Status | Account: Type |
| Last Name | Contact: Last Name |
| Mobile Phone | Contact: Mobile Phone |
| Note | Does not import |
| Phone | Contact: Phone and
Account: Phone |
| Phone Ext. | Contact: Business Phone Ext. |
| Referred By | Contact: Lead Source |
| Revenue | Account: Annual Revenue |
| State | Contact: Mailing State and
Account: Billing State |
| Ticker Symbol | Account: Ticker Symbol |
| Title | Contact: Title |
| Web Site | Account: Website |

| ACT! Field | Import Field |
|--|--|
| Zip | Contact: Mailing Postal Code
Account: Billing Postal Code |
| 2nd Contact | 2nd Contact: Name |
| 2nd Phone | 2nd Contact: Phone |
| 2nd Phone Ext. | 2nd Contact: Phone Ext. |
| 2nd Title | 2nd Contact: Title |
| 3rd Contact | 3rd Contact: Name |
| 3rd Phone | 3rd Contact: Phone |
| 3rd Phone Ext. | 3rd Contact: Phone Ext. |
| 3rd Title | 3rd Contact: Title |
| 2nd Last Reach, 3rd Last Reach, Asst. Title, Last Attempt, Last Meeting, Last Reach, Last Results, Letter Date, Pager, Spouse, User 1-15 | Contact: Note or Account: Note
(In Professional, Enterprise, Unlimited, Performance, and Developer Edition organizations, you specify which fields import into a single contact or account note; separate notes are not created for each ACT! field.) |

SEE ALSO:

[Export Contact Data from ACT!](#)

[Prepare Your Data for Import](#)

Default Field Mapping for Outlook

Outlook fields map to Salesforce account and contact import fields during an individual data import.

| Outlook Field | Import Field |
|-------------------|--|
| Assistant's Name | Contact: Assistant's Name |
| Assistant's Phone | Contact: Asst Phone |
| Birthday | Contact: Birthdate |
| Business City | Contact: Mailing City and
Account: Billing City |
| Business Country | Contact: Mailing Country and
Account: Billing Country |
| Business Fax | Contact: Fax and
Account: Fax |

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **All Editions** except **Database.com**

| Outlook Field | Import Field |
|--|---|
| Business Phone | Contact: Phone |
| Business Postal Code | Contact: Mailing Postal Code
Account: Billing Postal Code |
| Business Street | Contact: Mailing Address and
Account: Billing Address |
| Business Street 2 | Contact: Mailing Address and
Account: Billing Address |
| Business Street 3 | Contact: Mailing Address and
Account: Billing Address |
| Company | Account: Account Name and
Contact: Account |
| Company Main Phone | Account: Phone |
| Department | Contact: Department |
| E-mail | Contact: Email |
| (The import wizard verifies this is a valid email address in the form:
jsmith@acme.com) | |
| First Name | Contact: First Name |
| Home City | Contact: Other City |
| Home Country | Contact: Other Country |
| Home Phone | Contact: Home Phone |
| Home Postal Code | Contact: Other Postal Code |
| Home Street | Contact: Other Address |
| Home Street 2 | Contact: Other Address |
| Home Street 3 | Contact: Other Address |
| Job Title | Contact: Title |
| Last Name | Contact: Last Name |
| Manager's Name | Contact: Reports To

(In addition, if the name in this field does not match an existing contact, a new contact is created with the manager's name.) |
| Mobile Phone | Contact: Mobile Phone |

| Outlook Field | Import Field |
|---|---|
| Notes | Contact: Description |
| Other Phone | Contact: Other Phone |
| Referred By | Contact: Lead Source |
| Title | Contact: Salutation |
| Web Page | Account: Website |
| Account, Anniversary, Billing Information, Business Phone 2, Callback, Car Phone, Categories, Children, Directory Server, E-mail 2, E-mail 3, Government ID Number, Hobby, Home Fax, Home Phone 2, Internet Free/Busy Address, ISDN, Keywords, Language, Location, Middle Name, Mileage, Office Location, Organizational ID Number, Other City, Other Country, Other Fax, Other Postal Code, Other State, Other Street, Other Street 2, Other Street 3, Pager, PO Box, Primary Phone, Profession, Radio Phone, Spouse, Suffix, Telex, TTY/TDD Phone, User 1, User 2, User 3, User 4 | Contact: Note or Account: Note
(In Professional, Enterprise, Unlimited, Performance, and Developer Edition organizations, you specify which fields import into a single contact or account note; separate notes are not created for each Outlook field.) |

SEE ALSO:

[Export from Outlook](#)

[Prepare Your Data for Import](#)

Field Mapping for Other Data Sources and Organization Import

If you are importing accounts and contacts for an organization, or importing individual data from sources other than Outlook or ACT!, the Import Wizards map the fields as correctly as possible.

You must fine-tune the mapping before completing the import. Before importing your data, Salesforce recommends that you use Excel to label the columns in your import file with the labels listed below. Field length limits for each object are listed in the [Salesforce Field Reference Guide](#).

 **Note:** The default mappings listed below are offered as a guide for importing; they do not ensure 100% accuracy in mapping your data. You must fine-tune the mapping in the Import Wizards. Remember that you can map the same field multiple times if necessary—for example, for the account and contact address fields.

Common Fields for Contacts and Accounts

| Label for Your Import File | Salesforce Field |
|----------------------------|--|
| Record Owner | Contact: Contact Owner and
Account: Account Owner |

(Note: For individual imports, this field is not necessary, since all data you import is

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions** except **Database.com**

Organization import not available in: **Personal Edition**, **Database.com**

Common Fields for Contacts and Accounts

| Label for Your Import File | Salesforce Field |
|---|--|
| <p>automatically owned by you. In addition, when importing records by Salesforce record ID, this field is ignored.)</p> | |
| Currency ISO Code | Contact: Contact Currency and
Account: Account Currency |
| (Note: You can use this field only for organization imports in organizations that use multiple currencies.) | |

Contact Fields

| Label for Your Import File | Salesforce Field |
|---|---|
| Assistant | Contact: Assistant |
| Asst. Phone | Contact: Asst. Phone |
| Asst. Phone Ext. | Appended to Contact: Asst. Phone |
| Birthdate | Contact: Birthdate |
| Business Fax | Contact: Fax |
| Business Fax Ext. | Appended to Contact: Fax |
| Business Phone | Contact: Phone |
| Business Phone Ext. | Appended to Contact: Phone |
| Contact Description | Contact: Description |
| Contact Full Name <i>or</i>
First Name & Last Name | Contact: First Name and
Contact: Last Name |
| (Note: When importing contact names, use either Contact Full Name or First Name and Last Name, but not both.) | |
| Contact ID | Contact: Contact ID |
| (Note: Record IDs are case-sensitive and should not be changed.) | |
| Contact Note | Creates a note attached to the contact |
| Department | Contact: Department |
| E-mail Address | Contact: Email |
| (Note: The import wizard verifies this is a valid email address in the form: jsmith@acme.com.) | |
| Email Opt Out | Contact: Email Opt Out |

Contact Fields

| Label for Your Import File | Salesforce Field |
|---|--|
| (Note: Use "1" to indicate that user opts out; use "0" to indicate that user wants emails.) | |
| Home Phone | Contact: Home Phone |
| Home Phone Ext. | Appended to Contact: Home Phone |
| Lead Source | Contact: Lead Source |
| Mailing City | Contact: Mailing City |
| Mailing Country | Contact: Mailing Country |
| Mailing Postal Code | Contact: Mailing Address Zip/Postal Code |
| Mailing State | Contact: Mailing State/Province |
| Mailing Street 1 | Contact: Mailing Address |
| Mailing Street 2 | Contact: Mailing Address |
| Mailing Street 3 | Contact: Mailing Address |
| Mobile Phone | Contact: Mobile |
| Mobile Phone Ext. | Appended to Contact: Mobile |
| Other City | Contact: Other City |
| Other Country | Contact: Other Country |
| Other Phone | Contact: Other Phone |
| Other Phone Ext. | Appended to Contact: Other Phone |
| Other Postal Code | Contact: Other Address Zip/Postal Code |
| Other State | Contact: Other State/Province |
| Other Street 1 | Contact: Other Address |
| Other Street 2 | Contact: Other Address |
| Other Street 3 | Contact: Other Address |
| Reports To | Contact: Reports To |
| (Note: If the import wizard cannot find a contact that matches the name in this field, it will create a new contact using this value as the Contact: First Name & Last Name.) | |
| Salutation | Prefixed to Contact: First Name |
| Title | Contact: Title |

Contact Fields

| Label for Your Import File | Salesforce Field |
|-----------------------------------|---|
| 2nd Contact | Split into Contact: <code>First Name</code> & <code>Last Name</code> for a second contact for the account |
| 2nd Phone | Contact: <code>Phone</code> for a second contact for the account |
| 2nd Phone Ext. | Appended to Contact: <code>Phone</code> for a second contact for the account |
| 2nd Title | Contact: <code>Title</code> for a second contact for the account |
| 3rd Contact | Split into Contact: <code>First Name</code> & <code>Last Name</code> for a third contact for the account |
| 3rd Phone | Contact: <code>Phone</code> for a third contact for the account |
| 3rd Phone Ext. | Appended to Contact: <code>Phone</code> for a third contact for the account |
| 3rd Title | Contact: <code>Title</code> for a third contact for the account |

Account Fields

| Label for Your Import File | Salesforce Field |
|--|---|
| Account Description | Account: <code>Description</code> |
| Account Division | Account: <code>Account Division</code> |
| (Note: You do not need to specify this field if you choose to assign the division via the drop-down list on Step 1 of the import wizard. If you do not map this field or use the division drop-down list, the division is set to the record owner's default division for each record.) | |
| Account Fax | Account: <code>Fax</code> |
| Account Fax Ext. | Appended to Account: <code>Fax</code> |
| Account ID | Account: <code>Account ID</code> |
| (Note: Record IDs are case-sensitive and should not be changed.) | |
| Account Name | Account: <code>Account Name</code> and
Contact: <code>Account</code> |
| Account Note | Creates a note attached to the account |
| Account Number | Account: <code>Account Number</code> |
| Account Phone | Account: <code>Phone</code> |
| Account Phone Ext. | Appended to Account: <code>Phone</code> |
| Account Site | Account: <code>Account Site</code> |
| Account Type | Account: <code>Type</code> |

Account Fields

| Label for Your Import File | Salesforce Field |
|--|---|
| Billing City | Account: Billing City |
| Billing Country | Account: Billing Country |
| Billing Postal Code | Account: Billing Zip/Postal Code |
| Billing State | Account: Billing State/Province |
| Billing Street 1 | Account: Billing Address |
| Billing Street 2 | Account: Billing Address |
| Billing Street 3 | Account: Billing Address |
| Employees | Account: Employees |
| Industry | Account: Industry |
| Ownership | Account: Ownership |
| Parent Account | Account: Parent Account |
| (Note: If the import wizard cannot find an account that matches the parent account name, it will create a new account using this value as the Account Name.) | |
| Parent Account Site | Account: Account Site |
| (Note: Indicates the site value of Parent Account.) | (Note: Maps to the Account Site field in the parent account.) |
| Rating | Account: Rating |
| Revenue | Account: Annual Revenue |
| Shipping City | Account: Shipping City |
| Shipping Country | Account: Shipping Country |
| Shipping Postal Code | Account: Shipping Zip/Postal Code |
| Shipping State | Account: Shipping State/Province |
| Shipping Street 1 | Account: Shipping Address |
| Shipping Street 2 | Account: Shipping Address |
| Shipping Street 3 | Account: Shipping Address |
| SIC Code | Account: SIC Code |
| Ticker Symbol | Account: Ticker Symbol |
| Website | Account: Website |

 **Note:** If you include record types in your import file, the Import Wizard uses the record owner's default record type when creating new records. For existing records, the Import Wizard does not update the record type field.

SEE ALSO:

[Prepare Your Data for Import](#)

Field Mapping for Importing Leads

To improve the accuracy of your import, label the columns in your import file to match the Salesforce Lead fields. When you import the leads, the Data Import Wizard maps the fields in your import file

 **Note:** The following default mappings aren't always 100% accurate in mapping your data. Check the import and fine-tune the mapping in the Data Import Wizard as necessary.

| Import File Label | Salesforce Lead Field |
|---|--------------------------|
| Annual Revenue | Annual Revenue |
| City | City |
| Company | Company |
| Country | Country |
| Currency ISO Code | Lead Currency |
| Note: Use this field only for orgs that use multiple currencies; see Rules for Importing Multiple Currencies on page 685. | |
| Description | Description |
| Email | Email |
| The Data Import Wizard verifies email addresses in the form of jsmith@acme.com. | |
| Email Opt Out | Email Opt Out |
| Use "1" to indicate that the user opts out. Use "0" to indicate that the user wants emails. | |
| No. of Employees | No. of Employees |
| Fax | Fax |
| Full Name or First Name & Last Name | First Name and Last Name |
| (Note: When importing lead names, use either Full Name or First Name and Last Name, but not both.) | |
| Industry | Industry |

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer Editions

| Import File Label | Salesforce Lead Field |
|--|--|
| Lead Division
Note: Do not specify this field if you assign the division using the dropdown list in Step 1 of the Data Import Wizard. If you do not map this field or use the division dropdown list, the division is set to the record owner's default division for each record. | Lead Division |
| Lead ID
Note: Record IDs are case-sensitive and must not be changed. | Lead ID |
| Lead Source
Note: Do not specify this field if you assign the same lead source to all leads on the first page of the Data Import Wizard. The Lead Source dropdown lists all active lead source picklist values. | Lead Source |
| Lead Status | Lead Status |
| Mobile Phone | Mobile |
| Phone | Phone |
| Postal Code | Postal Code |
| Rating | Rating |
| Record Owner
Note: You do not need this field if you assign ownership using a lead assignment rule. When you import records by Salesforce record ID, this field is ignored. | Lead Owner |
| Salutation | Added to beginning of First Name |
| State | State |
| Status | Status
(in the Campaign History related list of a lead) |
| Street 1 | Address |
| Street 2 | Address |
| Street 3 | Address |
| Title | Title |
| Website | Website |

If you include record types in this list, the Data Import Wizard uses the record owner's default record type when creating new records. For existing records, the Data Import Wizard does not update the record type field.

If you use assignment rules, the Data Import Wizard uses the new owner's default record type when creating new records. When the assignment rules assign the record to a queue, the queue owner's default record type is used.

SEE ALSO:

[Prepare Your Data for Import](#)

Data Import Wizard

The Data Import Wizard makes it easy to import data for many standard Salesforce objects, including accounts, contacts, leads, solutions, campaign members, and person accounts. You can also import data for custom objects. You can import up to 50,000 records at a time.

Salesforce recommends that you test a small file first to make sure that you prepared your source data correctly.

These browsers support the Data Import Wizard:

- Chrome™ version 29 and later
- Mozilla® Firefox® version 23 and later
- Microsoft® Internet Explorer® version 9 and later
- Apple® Safari® version 5 and later
- Internet Explorer 9 doesn't support dragging CSV files into the browser.
- Don't run more than one import job at a time, even from separate browser windows.
- Data Import Wizard doesn't support importing custom objects into Experience Cloud sites.

SEE ALSO:

[Import Data with the Data Import Wizard](#)

Import Data with the Data Import Wizard

After preparing your data for import, use the Data Import Wizard to map the data fields and run the import.

1. Prepare your data for import and create an import file. Doing this step first prevents errors, duplication of data, and frustration.

For more information, see the FAQ item "How do I prepare my data for import?" on the Data Import wizard welcome page.

You can also view the following video playlist to get more information: [Data Import How To Series](#)

2. To start the wizard, from Setup, enter *Data Import Wizard* in the Quick Find box, then select **Data Import Wizard**.
3. Review the information provided on the welcome page, then click **Launch Wizard**.
You can also launch the Data Import Wizard from the Tools list on the object-specific home page. Users who aren't administrators can also access the Data Import wizard from their personal settings.
4. Choose the data that you want to import.

EDITIONS

Available in: Salesforce Classic (**not available in all orgs**) and Lightning Experience

Available in: **All Editions** except **Database.com**

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **All** except **Database.com** and **Personal Editions**

USER PERMISSIONS

To import data with the Data Import Wizard:

- Depends on what you're importing. See [What permissions do I need to import records?](#) in Salesforce Help .

- a. To import accounts, contacts, leads, solutions, person accounts, or articles, click **Standard Objects**. To import custom objects, click **Custom Objects**.
 - b. Specify whether you want to add new records to Salesforce, update existing records, or add and update records simultaneously. If you have workflows that add new objects when importing, selecting **add new and update existing records** fires them, but selecting **update existing records** doesn't.
 - c. Specify matching and other criteria as necessary. Hover your mouse over the question marks for more information about each option. For updates and upserts of custom objects, match by Name is case-sensitive.
 - d. Specify whether to trigger workflow rules and processes when the imported records meet the criteria.
 - e. Specify the file that contains your data by dragging the CSV file to the upload area of the page. You can also click the CSV category you're using and then navigate to the file..
 - f. Choose a character encoding method for your file. Typically, you don't change your character encoding.
 - g. Select comma or tab as a value separator.
 - h. Click **Next**.
5. Map your data fields to Salesforce data fields. The Data Import wizard maps as many of your data fields as possible to standard Salesforce data fields. But if the wizard can't map fields, you must do it manually. Unmapped fields are not imported into Salesforce. To see a list of standard Salesforce data fields, from the management settings for the object, go to the fields area.
- a. Scan the list of mapped data fields and locate the unmapped fields.
 - b. Click **Map** to the left of each unmapped field.
 - c. In the Map Your Field dialog box, search and choose up to 10 Salesforce fields to map to and click **Map**. You also have the option to save data from unmapped fields in a general notes field for accounts and contacts. Choose **Account Note** or **Contact Note** from the Map To dropdown list and click **Map**.
 - d. To change mappings that Salesforce performed automatically, click **Change** to the left of the appropriate field. Delete the Salesforce fields you don't want to map, choose the fields you want to map, then click **Map**.
 - e. Click **Next**.
6. Review your import information on the Review page. If you still have unmapped fields that you want to import, click **Previous** to return to the previous page and specify your mappings.
7. Click **Start Import**.
8. Check import status.

The **Recent Import Jobs** chart on the Data Import Wizard home page lists the status and metrics of the data import. Alternately from Setup, enter *Bulk Data Load Jobs* in the Quick Find box, then select **Bulk Data Load Jobs**. The Bulk Data Load Jobs page is not available in Professional Edition. Only administrators have access to the Bulk Data Load Jobs page in Salesforce Setup. If you're not an administrator, you can check the status of your upload by monitoring the relevant tabs in Salesforce.

Need help with getting started? Check out www.salesforce.com/gettingstarted to access live webinars, videos, setup series and more. For hands-on help with data importing, complete the [Importing Data](#) module in Trailhead.

Add Person Accounts with the Data Import Wizard

To add person accounts to your Salesforce org, launch the Data Import Wizard from the accounts home page.

Before you begin, make sure that your import file is in CSV format and contains values for these fields.

- First Name
- Last Name
- Email
- Phone

 **Tip:** To obtain Salesforce IDs or other values from your org, run reports and then export the report data.

These steps describe one recommended method of importing data. You can import data into Salesforce fields that aren't listed here. You can also customize your import by using other options that appear in the Data Import Wizard.

1. From the accounts home page, click **Import Person Accounts**.
The Data Import Wizard appears.
2. Select **Person Accounts**, then select **Add new and update existing records**.
3. Set **Match Account by** to **Email**.
4. Select the CSV file that contains your import data, and click **Next**.
5. Map column headers from your CSV file to these fields.
 - First Name
 - Last Name
 - Email
 - Phone
6. Click **Next**.
7. Review the import settings, and then click **Start Import**.

When we finish importing your data, we notify you by email. Review the results and resolve any errors that occurred.

EDITIONS

Data Import Wizard available in both Salesforce Classic and Lightning Experience

Data Import Wizard available in **All** Editions except Database.com

Person accounts available in: both Salesforce Classic and Lightning Experience

Person accounts available in **Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To create person accounts that you own via the Data Import Wizard:

- Create on accounts
AND
Edit on accounts
AND
Import Personal Contacts

To create person accounts owned by others via the Data Import Wizard:

- Create on accounts
AND
Edit on accounts and contacts
AND
Modify All Data

Data Loader

Data Loader is a client application for the bulk import or export of data. Use it to insert, update, delete, or export Salesforce records. When importing data, Data Loader reads, extracts, and loads data from comma-separated values (CSV) files or from a database connection. When exporting, Data Loader outputs CSV files.

 **Important:** Data Loader documentation is in the [Salesforce Developer Portal](#).

Data Loader can be used on either MacOS or Windows, and offers these key features.

- An easy-to-use wizard interface for interactive use
- An alternative command-line interface for automated batch operations (Windows only)
- Support for large files with up to 5 million records
- Drag-and-drop field mapping
- Support for all objects, including custom objects
- Process data in both Salesforce and Database.com
- Detailed success and error log files in CSV format
- A built-in CSV file viewer

You can use Data Loader in two different ways:

- User interface—Specify configuration parameters and CSV files used for import and export, and define field mappings that map field names in your import file to field names in Salesforce.
- Command line (Windows only)—Specify the configuration, data sources, mappings, and actions in files. The command line enables you to set up Data Loader for automated processing.

 **Important:** Data Loader documentation is in the [Salesforce Developer Portal](#).

Undoing an Import

If you import accounts, contacts, leads, or solutions by mistake, your administrator can delete the items you mistakenly imported.

1. As the administrator, enter *Mass Delete Records* in the **Quick Find** box from Setup,
2. Select **Mass Delete Records** to delete the items were mistakenly imported. View the [Using Mass Delete to Undo Imports](#) document for instructions.

The Mass Delete Records tools do not support custom objects. If you import custom objects by mistake in Enterprise, Unlimited, Performance, or Developer Edition, your administrator can use the Data Loader to mass delete the mistakenly imported records.

SEE ALSO:

- [Data Import Wizard](#)
- [Import Data Into Salesforce](#)

Import Limits

Limits for importing data depend on the type of record.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** editions

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions** except **Database.com**

USER PERMISSIONS

User Permissions Needed

To mass delete data:

- **Modify All Data**

You can import data from ACT!, Outlook, and any program that can save data in the CSV (comma-separated values) format, such as Excel or GoldMine.

| Type of record | Import record limit | User permissions needed |
|---|--|--|
| Business accounts and contacts owned by you | 50,000 at a time via the Data Import Wizard | Import Personal Contacts |
| Business accounts and contacts owned by other users | 50,000 at a time | Modify All Data |
| Person accounts owned by you | 50,000 at a time | Create on accounts
AND
Edit on accounts
AND
Import Personal Contacts |
| Person accounts owned by other users | 50,000 at a time | Create on accounts
AND
Edit on accounts and contacts
AND
Modify All Data |
| Leads | 50,000 at a time | Import Leads |
| Campaign members | 50,000 at a time | Depends on what's being imported: <ul style="list-style-type: none"> • Campaign member statuses • Existing contacts • Existing leads • Existing person accounts • New contacts • New leads |
| Custom object | 50,000 at a time | Import Custom Objects
AND
Create on the custom object
AND
Edit on the custom object |
| Solutions | 50,000 at a time | Import Solutions |
| Assets | You can't import these records via the Data Import Wizard. | |
| Cases | | |
| Campaigns | | |

| Type of record | Import record limit | User permissions needed |
|----------------|---------------------|-------------------------|
| Contracts | | |
| Documents | | |
| Opportunities | | |
| Products | | |

- Your import file can be up to 100 MB, but each record in your file can't exceed 400 KB, which is about 4,000 characters. To determine how many fields you can import, use this formula: $4,000 / (\text{average number of characters in an API field name} * 2)$. For example, if your average field character length is 40, you can import approximately 50 fields.
- You can import up to 90 fields per record.
- Each imported note and each imported description can't exceed 32 KB. Text longer than 32 KB is truncated.
- Other Bulk API limits apply. If you have missing records or truncated fields due to limits, see [Bulk API Limits](#) in the Bulk API 2.0 and Bulk API Developer Guide.

Assets, cases, campaigns, contracts, documents, opportunities, and products can't be imported via import wizards.

General Importing Questions

Find answers to frequently asked questions about importing data and the Data Import Wizard.

[Who can use the Data Import Wizard?](#)

You can use the Data Import Wizard to import accounts, contacts, leads, solutions, person accounts, campaign members, and custom objects for multiple users at the same time.

[What permissions do I need to import records?](#)

You need different permissions to import records with Data Loader and Data Import Wizard.

[Why can't I log into Data Loader?](#)

If you're having trouble logging in to Data Loader, there are a few solutions to try.

[Who can import campaign members?](#)

Only users with the required permissions can import campaign members with the Data Import Wizard.

[Can I mass upload data into Salesforce?](#)

Group, Professional, Performance, Unlimited, Enterprise, and Developer editions allow you to mass upload data using the Data Import Wizard. From Setup, enter *Data Import Wizard* in the Quick Find box, then select **Data Import Wizard**. In addition, Performance, Unlimited, Enterprise, and Developer editions have API access to use database mass upload tools like Data Loader.

[Should I sync Outlook or use import wizards to upload my data into Salesforce?](#)

Use this information to determine how to upload data into Salesforce.

[Which data can I import?](#)

You can use the Data Import Wizard to import campaign member status, contacts and business accounts, person accounts, leads, solutions, and custom objects, depending on your Salesforce edition.

[How large can my import file be?](#)

Your import file can be up to 100 MB, but other size limits apply.

[How do I perform mass updates to records?](#)

To update more than 50,000 records but less than 5 million records, use Data Loader.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions.**

What file formats can the import wizards handle?

You can import contacts and business accounts directly from an ACT! or Outlook file, or from any CSV (comma-separated values) file, such as a GoldMine or Excel file. You can import leads, solutions, custom objects, or person accounts from any CSV file.

Why is there a delay in importing my file?

To manage the volume of imports and ensure that all users receive the highest level of performance, org import files are accepted in asynchronous mode. Your file passes through a controlled queue and is imported when the system can best manage the data, however your org import doesn't take longer than 24 hours to complete. You receive an email notification when the import is complete.

Can I do simultaneous imports?

The Data Import Wizard doesn't support simultaneous—or concurrent—data import jobs, even from separate browser windows. Finish one data import before beginning the next.

How long does it take to complete an import?

The time it takes to complete an import using the Data Import Wizard varies, depending on the amount of data you're importing. Imports can take up to several minutes.

How many records can I import?

You can import up to 50,000 records at a time with the Data Import Wizard.

What kind of objects can I import?

You can use the Data Import Wizard to import accounts, contacts, leads, solutions, campaign members, person accounts, and custom objects.

Can I import into custom fields?

Yes. Your administrator must create the custom fields before import. For checkbox fields, records with a value of *1* in the field are imported as checked, while a value of *0* is not checked.

Can I import into fields that are not on my page layout?

No, except for contacts. You can import values into a field only if you have read and edit access. User permissions, page layout assignments, and field-level security settings determine field access. The page layout used is based on the running user's selected record type.

Can I import data into a picklist field if the values don't match?

We recommend that you import your data into an existing picklist when that picklist accurately represents your data, even if the exact values don't match. The import wizards warn you before importing any new picklist values. However, the wizards accept any value for a picklist field, even if the value isn't predefined. Your administrator can later edit the picklist to include the needed values. Note that import wizards don't allow you to import more than 100 new picklist or multi-select picklist values for any field during a single import.

Can I delete my imported data if I make a mistake?

From Setup, your administrator can enter *Mass Delete Records* in the Quick Find box, then select **Mass Delete Records** to perform a mass delete of accounts, contacts, leads, or solutions that you mistakenly imported. You cannot mass delete mistakenly imported custom objects.

How do I use the Data Import Wizard to update records that match specified Salesforce IDs?

You can use the Data Import Wizard to update leads, contacts, or accounts using the record's ID as the unique identifier. These steps don't apply to custom objects.

[Where Does Data Import Wizard Obtain the Country for the Country Field?](#)

The Country column is a mandatory field and if it is not provided in your comma-separated values (CSV) file, Data Import Wizard tries to derive it from other sources. This action avoids any insert issues when, for example, the CSV file has a State column but no Country column. For the value, Data Import Wizard checks to see if the Default Country/Territory is specified in the State and Country/Territory Picklists. If a country is selected from the picklist, then Data Import Wizard uses that value for the Country. If a country is not selected, then the country selected in Signup Country Code during the org sign-up is used.

[How do I update fields with blank values?](#)

To replace fields with null values, you must use Data Loader.

[Can I bulk-assign records to a record type?](#)

Yes, you can bulk-assign records to a record type using the Data Import Wizard. You choose to which record type to assign the records during the import process. This process applies to standard and custom objects.

[How many campaign members can I import?](#)

With the Data Import Wizard, your import file can have up to 50,000 record rows. Your imports are also subject to the overall storage limits for your org.

[What status is assigned to campaign members?](#)

With the Data Import Wizard, you can map a column in your import file to the `Status` field. Blank or invalid status values are set to the default status.

[Can I import using external IDs?](#)

When importing custom objects, solutions, or person accounts, you can use external IDs to prevent the import from creating duplicate records.

[Can I match lookups and master-detail records using external IDs?](#)

Yes, using the Data Import Wizard, you can choose from multiple external IDs to match to lookups and master-detail records.

[Why doesn't Data Loader import special characters?](#)

If Data Loader fails to import special characters such as ö, ñ, or é, your source data file isn't properly encoded.

[Why do date fields import incorrectly when I use the Data Loader?](#)

Sometimes dates import incorrectly because the Data Loader converts the date specified in the imported .csv file to GMT. If your machine's time zone isn't GMT or if your machine's clock adjusts for daylight savings time (DST), your dates can be off by a day.

[Can I import amounts in different currencies?](#)

If your Group, Professional, Enterprise, Unlimited, Performance, or Developer Edition org has set up the ability to use multiple currencies, you can import amounts in different currencies using the Currency ISO Code column in your import file.

[Can I import data in more than one language?](#)

The import wizard imports one language at a time, the language of the user doing the import. If you have the same data in different languages, run an import for each additional language.

[Can Customer Support help me import my data?](#)

Customer Support is available to assist Group, Contact Manager, Professional, Enterprise, Unlimited, and Performance Edition orgs throughout the import process.

Who can use the Data Import Wizard?

You can use the Data Import Wizard to import accounts, contacts, leads, solutions, person accounts, campaign members, and custom objects for multiple users at the same time.

- In Personal Edition, the Data Import Wizard isn't available.
- In Contact Manager Edition, you can't import leads and solutions with the Data Import Wizard.

- In Group Edition and Essentials Edition, you can't import solutions with the Data Import Wizard.
- In communities, you can't import custom objects with the Data Import Wizard.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small windows, while the Data Import Wizard opens in a full browser with `dataimporter.app` at the end of the URL. From Setup, enter *Data Import Wizard* in the *Quick Find* box, then select **Data Import Wizard**. The options you see depend on your permissions.

What permissions do I need to import records?

You need different permissions to import records with Data Loader and Data Import Wizard.

Data Loader

Importing records with Data Loader requires these permissions.

- "Read," "Create," "Edit," and "Delete" on the objects
- "API Enabled"
- "Bulk API Hard Delete" (only if you configure Data Loader to use Bulk API to hard-delete records)

Data Import Wizard

| Import Option | User Permissions Needed |
|---|--|
| To import accounts and contacts that you own via the Data Import Wizard: | Import Personal Contacts |
| To import accounts and contacts owned by others via the Data Import Wizard: | Modify All Data |
| To import leads via the Data Import Wizard: | Import Leads |
| To import custom object data via the Data Import Wizard: | Import Custom Objects
AND
Create on the custom object |
| To import solutions via the Data Import Wizard: | Import Solutions |
| To add or update campaign members via the Data Import Wizard: | Marketing User selected in your user information
AND
Read on contacts OR Import Leads
AND
Edit on campaigns |
| To add contacts that you own to a campaign via the Data Import Wizard: | Marketing User selected in your user information
AND
Create on accounts
AND |

Import Option**User Permissions Needed**

| | |
|---|--|
| | <p>Read on contacts</p> <p>AND</p> <p>Edit on accounts and campaigns</p> <p>AND</p> <p>Import Personal Contacts</p> |
| To create contacts that you own and add them to a campaign via the Data Import Wizard: | <p>Marketing User selected in your user information</p> <p>AND</p> <p>Create on accounts</p> <p>AND</p> <p>Read on contacts</p> <p>AND</p> <p>Edit on accounts and campaigns</p> <p>AND</p> <p>Import Personal Contacts</p> |
| To add contacts owned by others to a campaign via the Data Import Wizard: | <p>Marketing User selected in your user information</p> <p>AND</p> <p>Create on accounts</p> <p>AND</p> <p>Read on contacts</p> <p>AND</p> <p>Edit on accounts, contacts, and campaigns</p> <p>AND</p> <p>Modify All Data</p> |
| To create contacts owned by others and add them to a campaign via the Data Import Wizard: | <p>Marketing User selected in your user information</p> <p>AND</p> <p>Create on accounts</p> <p>AND</p> <p>Read on contacts</p> <p>AND</p> <p>Edit on accounts, contacts, and campaigns</p> <p>AND</p> <p>Modify All Data</p> |
| To add existing leads to a campaign via the Data Import Wizard: | <p>Marketing User selected in your user information</p> <p>AND</p> |

| Import Option | User Permissions Needed |
|--|--|
| | Edit on campaigns
AND
Import Leads |
| To create leads and add them to a campaign via the Data Import Wizard: | Marketing User selected in your user information
AND
Edit on campaigns
AND
Import Leads |
| To add person accounts that you own to a campaign via the Data Import Wizard: | Create on accounts
AND
Edit on accounts
AND
Import Personal Contacts |
| To create person accounts that you own via the Data Import Wizard: | Create on accounts
AND
Edit on accounts
AND
Import Personal Contacts |
| To add person accounts owned by others to a campaign via the Data Import Wizard: | Create on accounts
AND
Edit on accounts and contacts
AND
Modify All Data |
| To create person accounts owned by others via the Data Import Wizard: | Create on accounts
AND
Edit on accounts and contacts
AND
Modify All Data |

 **Important:** Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small windows, while the Data Import Wizard opens in a full browser with `dataimporter.app` at the end of the URL. From Setup, enter *Data Import Wizard* in the Quick Find box, then select **Data Import Wizard**. The options you see depend on your permissions.

Why can't I log into Data Loader?

If you're having trouble logging in to Data Loader, there are a few solutions to try.

- Add a security token to the end of your password to log in to Data Loader.
- Change the `Server host` to point to the appropriate server in Data Loader by following these steps:
 1. Start the Data Loader.
 2. Navigate to **Settings > Settings**.
 3. Set `Server host` to `https://yourInstance.salesforce.com/`, where `instance_name` is the Salesforce instance you're on.
 4. Click **OK** to save your settings.
- Ask your administrator whether you're working behind a proxy server. If so, adjust your Data Loader settings. If you're using APIs that are behind a proxy server, the proxy server prevents the APIs from connecting with Salesforce servers; you don't see information about the APIs under Login History.
- Try to log in on another computer to verify that your local device settings aren't causing the problem.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

SEE ALSO:

[Set Trusted IP Ranges for Your Organization](#)

Who can import campaign members?

Only users with the required permissions can import campaign members with the Data Import Wizard.

| Import Option | User Permissions Needed |
|--|--|
| To add or update campaign members via the Data Import Wizard: | <p>Marketing User selected in your user information</p> <p>AND</p> <p>Read on contacts OR Import Leads</p> <p>AND</p> <p>Edit on campaigns</p> |
| To add contacts that you own to a campaign via the Data Import Wizard: | <p>Marketing User selected in User Detail</p> <p>AND</p> <p>Create on accounts</p> <p>AND</p> <p>Read on contacts</p> <p>AND</p> <p>Edit on accounts and campaigns</p> <p>AND</p> <p>Import Personal Contacts</p> |

Import Option**User Permissions Needed**

To create contacts that you own and add them to a campaign via the Data Import Wizard:

Marketing User selected in User Detail
 AND
 Create on accounts
 AND
 Read on contacts
 AND
 Edit on accounts and campaigns
 AND
 Import Personal Contacts

To add contacts owned by others to a campaign via the Data Import Wizard:

Marketing User selected in User Detail
 AND
 Create on accounts
 AND
 Read on contacts
 AND
 Edit on accounts, contacts, and campaigns
 AND
 Modify All Data

To create contacts owned by others and add them to a campaign via the Data Import Wizard:

Marketing User selected in User Detail
 AND
 Create on accounts
 AND
 Read on contacts
 AND
 Edit on accounts, contacts, and campaigns
 AND
 Modify All Data

To add existing leads to a campaign via the Data Import Wizard:

Marketing User selected in User Detail
 AND
 Edit on campaigns
 AND
 Import Leads

| Import Option | User Permissions Needed |
|--|--|
| To create leads and add them to a campaign via the Data Import Wizard: | Marketing User selected in User Detail
AND
Edit on campaigns
AND
Import Leads |
| To add person accounts that you own to a campaign via the Data Import Wizard: | Create on accounts
AND
Edit on accounts
AND
Import Personal Contacts |
| To add person accounts owned by others to a campaign via the Data Import Wizard: | Create on accounts
AND
Edit on accounts and contacts
AND
Modify All Data |

Can I mass upload data into Salesforce?

Group, Professional, Performance, Unlimited, Enterprise, and Developer editions allow you to mass upload data using the Data Import Wizard. From Setup, enter *Data Import Wizard* in the Quick Find box, then select **Data Import Wizard**. In addition, Performance, Unlimited, Enterprise, and Developer editions have API access to use database mass upload tools like Data Loader.

Should I sync Outlook or use import wizards to upload my data into Salesforce?

Use this information to determine how to upload data into Salesforce.

- To upload accounts and contacts for multiple users at the same time, use the Data Import Wizard and select **Accounts and Contacts**.
- To upload your contacts from any application other than Microsoft Outlook, use the Data Import Wizard and select **Accounts and Contacts**.
- To keep your Outlook contacts, accounts, and calendar events up to date with Salesforce, use Lightning Sync or Salesforce for Outlook to initially sync and update your data.
- To upload custom objects, leads, person accounts, campaign members, and solutions, use the Data Import Wizard and select the appropriate object to import those kinds of records into Salesforce. You can't sync those records using Lightning Sync or Salesforce for Outlook.
- To upload business accounts and contacts for multiple users at the same time, use the Data Import Wizard and select **Accounts and Contacts**.

 **Note:** When you import person accounts, the following limitations apply.

- You can't upload person accounts with Salesforce for Outlook.

- You can sync contacts in Outlook to person accounts in Salesforce only if the person accounts exist. Syncing doesn't convert Outlook contacts to person accounts in Salesforce.

For more information about importing person accounts, see [Data Import Wizard](#) on page 702.

Which data can I import?

You can use the Data Import Wizard to import campaign member status, contacts and business accounts, person accounts, leads, solutions, and custom objects, depending on your Salesforce edition.

You can use import wizards to import these records.

- Campaign Member status
In Professional, Enterprise, Unlimited, Performance, and Developer Edition orgs, use the Data Import Wizard to import the status of campaign members.
- Contacts and business accounts
Use the Data Import Wizard to import contacts and business accounts.
In Professional, Enterprise, Unlimited, Performance, and Developer Edition orgs, you can also import contact and business account notes.
- Person accounts
In Professional, Enterprise, Unlimited, Performance, and Developer Edition orgs, use the Data Import Wizard to import person accounts.
- Leads
In Professional, Enterprise, Unlimited, Performance, and Developer Edition orgs, use the Data Import Wizard to import leads.
- Solutions
In Professional, Enterprise, Unlimited, Performance, and Developer Edition orgs, use the Data Import Wizard to import solutions.
- Custom objects
In Contact Manager, Group, Professional, Enterprise, Unlimited, Performance, and Developer Edition orgs, use the Data Import Wizard to import custom objects.

You can import values into a field only if you have read and edit access. User permissions, page layout assignments, and field-level security settings determine field access.

Import wizards for other records aren't available.

 **Important:** Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small windows, while the Data Import Wizard opens in a full browser with `dataimporter.app` at the end of the URL. From Setup, enter *Data Import Wizard* in the **Quick Find** box, then select **Data Import Wizard**. The options you see depend on your permissions.

How large can my import file be?

Your import file can be up to 100 MB, but other size limits apply.

- Your import file can be up to 100 MB, but each record in your file can't exceed 400 KB, which is about 4,000 characters. To determine how many fields you can import, use this formula: $4,000 / (\text{average number of characters in an API field name} * 2)$. For example, if your average field character length is 40, you can import approximately 50 fields.
- You can import up to 90 fields per record.

- Each imported note and each imported description can't exceed 32 KB. Text longer than 32 KB is truncated.
- Other Bulk API limits apply. If you have missing records or truncated fields due to limits, see [Bulk API Limits](#) in the Bulk API 2.0 and Bulk API Developer Guide.

Your import is also subject to your org's storage limit. The size of your import file doesn't directly correlate to the storage space needed for those records. For example, a 50 MB import file doesn't create 50 MB of data in Salesforce.

 **Important:** Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small windows, while the Data Import Wizard opens in a full browser with `dataimporter.app` at the end of the URL. From Setup, enter *Data Import Wizard* in the `Quick Find` box, then select **Data Import Wizard**. The options you see depend on your permissions.

How do I perform mass updates to records?

To update more than 50,000 records but less than 5 million records, use Data Loader.

To update more than 5 million records, we recommend you work with a Salesforce partner or visit the [AppExchange](#) for a suitable partner product.

What file formats can the import wizards handle?

You can import contacts and business accounts directly from an ACT! or Outlook file, or from any CSV (comma-separated values) file, such as a GoldMine or Excel file. You can import leads, solutions, custom objects, or person accounts from any CSV file.

 **Note:** If commas aren't appropriate for your locale, use a tab or other delimiter. Specify your delimiter in Data Loader Settings ([Settings](#) | [Settings](#)).

Why is there a delay in importing my file?

To manage the volume of imports and ensure that all users receive the highest level of performance, org import files are accepted in asynchronous mode. Your file passes through a controlled queue and is imported when the system can best manage the data, however your org import doesn't take longer than 24 hours to complete. You receive an email notification when the import is complete.

Can I do simultaneous imports?

The Data Import Wizard doesn't support simultaneous—or concurrent—data import jobs, even from separate browser windows. Finish one data import before beginning the next.

How long does it take to complete an import?

The time it takes to complete an import using the Data Import Wizard varies, depending on the amount of data you're importing. Imports can take up to several minutes.

If you're a Salesforce admin, you can check the status of an import on the Bulk Downloads page. From Setup, enter *Bulk Data Load Jobs* in the `Quick Find` box, then select **Bulk Data Load Jobs**.

If you're not a Salesforce admin, you can find the status of your import in the status email you receive. You can also monitor the import manually by checking the relevant tabs in Salesforce.

How many records can I import?

You can import up to 50,000 records at a time with the Data Import Wizard.

What kind of objects can I import?

You can use the Data Import Wizard to import accounts, contacts, leads, solutions, campaign members, person accounts, and custom objects.

Can I import into custom fields?

Yes. Your administrator must create the custom fields before import. For checkbox fields, records with a value of *1* in the field are imported as checked, while a value of *0* is not checked.

SEE ALSO:

[Import Data Into Salesforce](#)

Can I import into fields that are not on my page layout?

No, except for contacts. You can import values into a field only if you have read and edit access. User permissions, page layout assignments, and field-level security settings determine field access. The page layout used is based on the running user's selected record type.

 **Important:** Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small windows, while the Data Import Wizard opens in a full browser with `dataimporter.app` at the end of the URL. From Setup, enter *Data Import Wizard* in the **Quick Find** box, then select **Data Import Wizard**. The options you see depend on your permissions.

Can I import data into a picklist field if the values don't match?

We recommend that you import your data into an existing picklist when that picklist accurately represents your data, even if the exact values don't match. The import wizards warn you before importing any new picklist values. However, the wizards accept any value for a picklist field, even if the value isn't predefined. Your administrator can later edit the picklist to include the needed values. Note that import wizards don't allow you to import more than 100 new picklist or multi-select picklist values for any field during a single import.

 **Important:** Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small windows, while the Data Import Wizard opens in a full browser with `dataimporter.app` at the end of the URL. From Setup, enter *Data Import Wizard* in the **Quick Find** box, then select **Data Import Wizard**. The options you see depend on your permissions.

Can I delete my imported data if I make a mistake?

From Setup, your administrator can enter *Mass Delete Records* in the **Quick Find** box, then select **Mass Delete Records** to perform a mass delete of accounts, contacts, leads, or solutions that you mistakenly imported. You cannot mass delete mistakenly imported custom objects.

View the [Using Mass Delete to Undo Imports](#) document for instructions.

How do I use the Data Import Wizard to update records that match specified Salesforce IDs?

You can use the Data Import Wizard to update leads, contacts, or accounts using the record's ID as the unique identifier. These steps don't apply to custom objects.

 **Note:** These steps assume that you have an administrator-level of knowledge with Salesforce.

Before you begin, prepare the data you're updating.

1. Create a tabular report for the records you're updating, including the record ID and the fields you're updating.
2. Save the report locally as a .csv file for backup purposes.
3. To create a version of the .csv file and make your changes to the data, click **Save As**.
4. Click **Save**.

After you have updated the report, import the CSV file into Salesforce. The steps vary based on the records you're updating.

Update Leads

1. From Setup, enter *Data Import Wizard* in the Quick Find box, then select **Data Import Wizard**.
2. Click **Launch Wizard**.
3. Select **Leads**, then select **Update existing records**.
4. Set *Match Lead by* to Salesforce.com ID.
5. Select the CSV file that contains your import data, and click **Next**.
6. Map the *Lead ID* field to the Lead ID column in your CSV file, and map the other fields.
7. Click **Next**.
8. Review the import settings, and then click **Start Import**.

Update Accounts or Contacts

1. From Setup, enter *Data Import Wizard* in the Quick Find box, then select **Data Import Wizard**.
2. Click **Launch Wizard**.
3. Select **Accounts and Contacts**, then select **Update existing records**.
4. Set *Match Contact by* to Salesforce.com ID.
5. Set *Match Account by* to Salesforce.com ID.
6. Select *Update existing Account information*.
7. Select the CSV file that contains your import data, and click **Next**.
8. Map the contact ID, phone, and address fields to the relevant columns in your CSV file.
9. Map the account ID and other fields to the relevant columns in your CSV file.
10. Click **Next**.
11. Review the import settings, and then click **Start Import**.

The Data Import Wizard matches the record IDs in your file with the record IDs in Salesforce and updates the fields that were mapped.

SEE ALSO:

[Data Import Wizard](#)

Where Does Data Import Wizard Obtain the Country for the Country Field?

The Country column is a mandatory field and if it is not provided in your comma-separated values (CSV) file, Data Import Wizard tries to derive it from other sources. This action avoids any insert issues when, for example, the CSV file has a State column but no Country column. For the value, Data Import Wizard checks to see if the Default Country/Territory is specified in the State and Country/Territory Picklists. If a country is selected from the picklist, then Data Import Wizard uses that value for the Country. If a country is not selected, then the country selected in Signup Country Code during the org sign-up is used.

How do I update fields with blank values?

To replace fields with null values, you must use Data Loader.

1. To open Data Loader, choose **Start > All Programs > Salesforce > Data Loader > Data Loader**.
2. Click **Export** and complete the wizard. When the operation finishes, click **View Extraction**.
3. To open your data in Excel, click **Open in external program**. Blank out the fields you want to update.
4. In Data Loader, choose **Settings > Settings**, and select **Insert null values**. To save your settings, click **OK**.
5. To reimport your data, click **Update** and follow the instructions.

Can I bulk-assign records to a record type?

Yes, you can bulk-assign records to a record type using the Data Import Wizard. You choose to which record type to assign the records during the import process. This process applies to standard and custom objects.

 **Important:** Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small windows, while the Data Import Wizard opens in a full browser with `dataimporter.app` at the end of the URL. From Setup, enter *Data Import Wizard* in the `Quick Find` box, then select **Data Import Wizard**. The options you see depend on your permissions.

How many campaign members can I import?

With the Data Import Wizard, your import file can have up to 50,000 record rows. Your imports are also subject to the overall storage limits for your org.

What status is assigned to campaign members?

With the Data Import Wizard, you can map a column in your import file to the `status` field. Blank or invalid status values are set to the default status.

Can I import using external IDs?

When importing custom objects, solutions, or person accounts, you can use external IDs to prevent the import from creating duplicate records.

An external ID is a custom field that has the External ID attribute, meaning that it contains unique record identifiers from a system outside of Salesforce. When you select this option, the Data Import Wizard detects existing records in Salesforce with external IDs that match those values in the import file.

Can I match lookups and master-detail records using external IDs?

Yes, using the Data Import Wizard, you can choose from multiple external IDs to match to lookups and master-detail records.

Why doesn't Data Loader import special characters?

If Data Loader fails to import special characters such as ö, ñ, or é, your source data file isn't properly encoded.

To ensure that the file is properly encoded:

1. Modify your source data file in .xls format.
2. In Microsoft® Excel®, save a copy of your file as a Unicode Text file.
3. Open the Unicode Text file you saved with a text editor.
4. To change these file settings, click **File > Save As:**
 - File name extension—**.csv**
 - Save as type—**All Files**
 - Encoding—**UTF-8**

5. Click **Save**, and close the file.

 **Note:** Don't open the file after you have saved the settings or you can revert the encoding changes.

6. Import the data using Data Loader as you normally do, and select the newly created .csv file.

Why do date fields import incorrectly when I use the Data Loader?

Sometimes dates import incorrectly because the Data Loader converts the date specified in the imported .csv file to GMT. If your machine's time zone isn't GMT or if your machine's clock adjusts for daylight savings time (DST), your dates can be off by a day.

To prevent the Data Loader from adjusting the date when it converts to GMT, directly change the format of cells containing dates to reflect the native time zone.

1. Open your .csv file in Microsoft® Excel®.
2. In each cell in which you entered dates, add hour data to represent the native time zone. For example, if the date is June 9, 2011 and the time zone is GMT+8, enter *June 9, 2011 8:00*. Excel reformats this date to *6/9/2011 8:00*.
3. Right-click the cell in which you entered the dates, and click **Format Cells**.
4. Click **Number > Custom**.
5. In **Type**, enter *yyyy-mm-ddThh:mm:ss.sssZ*. For example, if the cell was *6/9/2011 8:00*, it's now *2011-06-09T08:00:00.00Z*.

Can I import amounts in different currencies?

If your Group, Professional, Enterprise, Unlimited, Performance, or Developer Edition org has set up the ability to use multiple currencies, you can import amounts in different currencies using the Currency ISO Code column in your import file.

Can I import data in more than one language?

The import wizard imports one language at a time, the language of the user doing the import. If you have the same data in different languages, run an import for each additional language.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small windows, while the Data Import Wizard opens in a full browser with `dataimporter.app` at the end of the URL. From Setup, enter *Data Import Wizard* in the `Quick Find` box, then select **Data Import Wizard**. The options you see depend on your permissions.

Can Customer Support help me import my data?

Customer Support is available to assist Group, Contact Manager, Professional, Enterprise, Unlimited, and Performance Edition orgs throughout the import process.

Export Backup Data from Salesforce

Your Salesforce org can generate backup files of your data on a weekly or monthly basis depending on your edition. You can export all your org's data into a set of comma-separated values (CSV) files.

Note: Users with the "Weekly Data Export" permission can view all exported data and all custom objects and fields in the Export Service page. This permission is granted by default only to the System Administrator profile because it enables wide visibility.

You can generate backup files manually once every 7 days (for weekly export) or 29 days (for monthly export). In Professional Edition and Developer Edition, you can generate backup files only every 29 days. You can schedule backup files to generate automatically at weekly or monthly intervals (only monthly intervals are available in Professional Edition and Developer Edition).

Heavy traffic can delay an export delivery. For example, assume that you schedule a weekly export to run until the end of the month, beginning April 1. The first export request enters the queue, but due to heavy traffic, the export isn't delivered until April 8. On April 7, when your second export request is scheduled to be processed, the first request is still in the queue. So, the second request isn't processed until April 14.

Note: Only active users can run export jobs. If an inactive user schedules an export, error emails are generated and the export doesn't run.

1. From Setup, enter *Data Export* in the `Quick Find` box, then select **Data Export** and **Export Now** or **Schedule Export**.

- The **Export Now** option prepares your files for export immediately. This option is only available if enough time has passed since your last export.
- The **Schedule Export** option allows you to schedule the export process for weekly or monthly intervals.

2. Select the desired encoding for your export file.

3. Select `Include images, documents, and attachments` and `Include Salesforce Files and Salesforce CRM Content document versions` to include these items in your export data.

Note: Including special content in the export increases data export processing time.

4. If you want to have spaces instead of carriage returns or line breaks in your export files, select `Replace carriage returns with spaces`. This selection is useful if you plan to use your export files for importing or other integrations.

5. If you're scheduling your export, select the frequency (only available for orgs with monthly exports), start and end dates, and time of day for your export.

EDITIONS

Available in: both Salesforce Classic (**not available in all orgs**) and Lightning Experience

Weekly export available in: **Enterprise, Performance, and Unlimited** Editions

Monthly export available in: **All** editions, except for Database.com

USER PERMISSIONS

To export data:

- Weekly Data Export

6. Under Exported Data, select the types of data to include in your export. If you aren't familiar with the terminology used for some of the types of data, we recommend that you select **Include all data**. Note the following:
 - Formula (derived) and roll-up summary fields are always excluded from exports.
 - If your org uses divisions, data from all divisions is included in the export.
 - If your org uses person accounts and you are exporting accounts, all account fields are included in the account data.
 - If your org uses person accounts and you are exporting contacts, person account records are included in the contact data. However, the contact data only includes the fields shared by contacts and person accounts.
 - For information on field limitations, see the [Salesforce Field Reference Guide](#).
 - The **Include all data** option selects all objects for export at the time the checkbox is selected. For a recurring scheduled export, be sure to reselect the **Include all data** option to include newly created objects.
7. Click **Start Export** or **Save**.

Salesforce creates a zip archive of CSV files and emails the user who scheduled the export when it's ready. The email address for this notification can't be changed. Exports complete as soon as possible, however we can't guarantee the date and time of completion. Large exports are broken up into multiple files. To download the zip file, follow the link in the email or click **Data Export**. Zip files are deleted 48 hours after the email is sent (not including weekends). For example, if the email is sent on a Friday, the .Zip file is deleted on Tuesday.

 **Note:** For security purposes, Salesforce can require users to pass a CAPTCHA user verification test to export data from their org. This simple text-entry test prevents malicious programs from accessing your org's data. To pass the test, users must correctly type the two words displayed in the overlay's text box. The words entered in the text box must be separated by a space.

 **Tip:** Ensure that any automated processes that process the export files rely on the column headings in the CSV files, rather than the position of the columns.

Backup Data Export Considerations

No Sandbox Support

The data export service isn't supported in sandboxes. You can request an export in your sandbox, but the export doesn't get processed and doesn't complete. The only way to remove the export request after it's been queued is to refresh your sandbox.

File Size Considerations

If the size of data in the org is large, multiple .zip archives are created. Each .zip archive file contains one or more .csv files and can be up to 512 MB (approximately). If the total size of exported data is greater than 512 MB, the export generates multiple .zip files.

Adjust Export Files

Depending on the encoding selected, you might have to make adjustments to the export file before viewing it. Use the following instructions that apply to the character encoding you selected.

- [View Unicode \(UTF-8\) Encoded Export Files](#)
- [View Unicode \(UTF-16, Big Endian\) Encoded Export Files](#)
- [View Unicode \(Little Endian\) Encoded Export Files](#)

View Unicode (UTF-8) Encoded Export Files

If you have Microsoft Excel 2003:

1. Open Microsoft Excel.
2. Click **File > New**.
3. Click **Data > Import External Data > Import Data**.
4. In the Microsoft Excel text import wizard, select the CSV file.
5. Select "Delimited" and choose the "Unicode (UTF-8)" option for File origin.
6. Click **Next**.
7. Select **Comma** in the Delimiters section and click **Finish**. You might be prompted to select a range of cells.

 **Note:** If commas aren't appropriate for your locale, use a tab or other delimiter. Specify your delimiter in Data Loader Settings (**Settings | Settings**).

8. Repeat these steps for each file.

If you have an earlier version of Microsoft Excel (pre-2003):

1. Open the file in Microsoft Excel.
2. Select **File > Save As**.
3. Save the file as type Web Page.
4. Select **Tools > Options > General** tab and click the **Web Options** button.
5. Select the Encoding tab, and then choose the "Unicode (UTF-8)" option.
6. To close the dialog boxes, click **OK**.
7. To save the file with selected encoding, select **File > Save**.
8. Repeat these steps for each file.

View Unicode (UTF-16, Big Endian) Encoded Export Files

Open the export files in a text editor that supports this character set. Microsoft Excel does not support this character set.

View Unicode (Little Endian) Encoded Export Files

1. Open the file in Microsoft Excel.
2. Click column A to highlight the entire first column.
3. Open the **Data** menu and choose **Text to Columns**.
4. Select the "Delimited" radio button and click **Next**.
5. Select "Comma" in the Delimiters section and click **Finish**.

 **Note:** If commas aren't appropriate for your locale, use a tab or other delimiter. Specify your delimiter in Data Loader Settings (**Settings | Settings**).

6. Repeat these steps for each file.

Transfer Records

USER PERMISSIONS

| | |
|---|--|
| To transfer multiple accounts, campaigns, contacts, contracts, and custom objects: | Transfer Record
AND
Edit on the object type |
| To transfer multiple leads: | Transfer Leads OR Transfer Record
AND
Edit on leads |
| To transfer multiple cases: | Transfer Cases OR Transfer Record
AND
Edit on cases
AND
Read and Transfer Record on related accounts |
| To transfer account, asset, case, contact, lead, note, opportunity, order, PersonAccount, ServiceContract, SalesTeam, or any custom object to an inactive user: | Update Records with Inactive Owners (API only)
AND
Edit on the object type |
| To transfer account, asset, case, contact, lead, note, opportunity, order, PersonAccount, ServiceContract, SalesTeam, or any custom object from an inactive user: | Update Records with Inactive Owners
AND
Transfer Leads OR Transfer Cases OR Transfer Leads OR Transfer Record (Classic only)
AND
Edit on the object type |

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **Contact Manager, Group, Professional, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

Accounts, Campaigns, Contacts, Contracts, Leads, and Cases aren't available in **Database.com**.

Contracts are available in: **Performance** and **Developer** Editions and in **Professional, Enterprise, and Unlimited** Editions with the Sales Cloud.

A record owner, or any user above the owner in the role or territory hierarchy, can transfer a single record to another user. With some objects, such as cases, leads, and campaigns, sharing can be used to grant a user access to transferring records. Depending on the type of object, record ownership can be transferred in multiple ways.

| Method | Available for |
|--|---|
| Transfer a single record | Accounts, campaigns, cases, contacts, contracts, leads, opportunities, and custom objects |
| Transfer multiple records by selecting the records from a list view and clicking Change Owner | Cases, leads, and custom objects, which can belong to either a user or a queue |
| Transfer multiple records using the Mass Transfer tool | Accounts, leads, and custom objects |

Ability to Change Ownership

- Users with the Modify All Data permission or the Modify All permission for the given object can transfer any record, regardless of who owns the record.
- To transfer a single record or multiple records from a list view, the new owner must have at least the Read permission on the object type. This rule doesn't apply if you use the mass transfer tool.
- In Salesforce Classic, APEX code can't be used to update lead record owners to inactive users, even when users have the "Set Audit Fields upon Record Creation" and "Update Records with Inactive Owners" permissions assigned to them.
- When territory management isn't enabled, to transfer ownership of any single record, a user must have the appropriate Edit permission. The user must also either own the record or be above the owner in the role hierarchy. In addition, when a case is related to an account, a user must have Read and Transfer Record permissions on the account.

The Public Full Access and Public Read/Write/Transfer sharing settings give all users with the appropriate Edit permission the ability to transfer ownership of that type of record.

- When territory management is enabled, you can enable users assigned to territories to transfer the accounts in their territories, even when they aren't the record owner.
- To transfer campaigns, users must also have **Marketing User** selected on their user record.
- To transfer accounts that have related contacts who are external users, you must have the Manage Roles or Manage External Users permission.
- To transfer ownership of a case, contact, or opportunity record, either:
 - The new owner must already have at least read access to its associated parent account via sharing features.
 - The user who is transferring the record must have the ability to share the associated parent account. The account owner, system administrators, users who are above the account owner in the role hierarchy, and users with the Modify All permission on accounts have this ability.

Otherwise, the ownership transfer can't be completed.

Changing Ownership for Portal Accounts

- To transfer a Partner account, you must have the Manage Users or Manage External Users permission.
- If you own a Customer Portal account, you can transfer the account to any user in your same role without special permissions. You can't transfer a Customer Portal account to a user with a higher or lower role.
- Partner accounts can only be transferred to users with the Manage External Users permission.
- To transfer a Portal account with both Customer and Partner Portal users, you must have the Manage Users permission.
- You can't assign an account with Customer Portal users to an owner who is a partner user.

SEE ALSO:

[Mass Transfer Records](#)

Mass Transfer Records

Use the Mass Transfer tool to transfer multiple accounts, leads, service contracts, and custom objects from one user to another.

To transfer any records that you don't own, you need the required user permissions and read sharing access on the records.

1. From Setup, in the Quick Find box, enter *Mass Transfer Records*, and then select **Mass Transfer Records**.
2. Click the link for the type of record to transfer.
3. Optionally, fill in the name of the existing record owner in the `Transfer from` field. For leads, you can transfer from users or queues.
4. In the `Transfer to` field, fill in the name of new record owner. For leads, you can transfer to users or queues.
5. If your organization uses divisions, select the **Change division...** checkbox to set the division of all transferred records to the new owner's default division.
6. When transferring accounts, you can:
 - Select **Transfer open opportunities not owned by the existing account owner** to transfer open opportunities owned by other users that are associated with the account.
 - Select **Transfer closed opportunities** to transfer closed opportunities associated with the account. This option applies only to closed opportunities owned by the account owner. Closed opportunities owned by other users aren't changed.
 - Select **Transfer open cases owned by the existing account owner** to transfer open cases that are owned by the existing account owner and associated with the account.
 - Select **Transfer closed cases** to transfer closed cases that are owned by the existing account owner and associated with the account.
 - Select **Keep Account Team** to maintain the existing account team associated with the account. If you want to remove the existing account team associated with the account, deselect this checkbox.
 - Select **Keep Opportunity Team on all opportunities** to maintain the existing team on opportunities associated with this account. Any opportunity splits are preserved, and split percentages are assigned to the previous owner transfer to the new one. If this box is unchecked, all opportunity team members and splits are deleted when the opportunity is transferred.

 **Note:** If you transfer closed opportunities, the opportunity team is maintained, regardless of this setting.
7. Enter search criteria that the records you're transferring must match. For example, search accounts in California by specifying *Billing State/Province equals CA*.
8. Click **Find**.

 **Note:** The 'Mass Transfer Records' tool allows up to 250 records at a time. To perform transfers over 250 records, use the Data Loader or another tool.
9. Select the checkbox next to the records that you want to transfer. To select all currently displayed items, check the box in the column header.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Essentials, Contact Manager, Group, Professional, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

Service Contracts available in: **Professional, Enterprise, Performance, Unlimited**, and **Developer** Editions with the Service Cloud

Accounts and Leads not available in: **Database.com**

USER PERMISSIONS

To mass transfer accounts and service contracts:

- Transfer Record
- AND
- Transfer Leads

To mass transfer custom objects:

- Transfer Record

To mass transfer leads:

- Transfer Leads OR Transfer Record

If duplicate records are found, you must select only one of the records to transfer. Transferring duplicate records results in an error.

Duplicate records can appear if you filter leads based on Campaign Member Status and a matching lead has the same campaign member status on multiple campaigns. For example, if you specify *Campaign Member Status equals Sent*, and a matching lead named John Smith has the status Sent on two campaigns, his record displays twice.

10. Click **Transfer**.

When you change record ownership, some associated items that are owned by the current record owner also transfer to the new owner.

| Record | Associated items that are also transferred |
|----------|---|
| Accounts | Contacts (on business accounts only), attachments, notes, open activities, open opportunities owned by the current account owner, and optionally, closed opportunities and open opportunities owned by other users. |
| Leads | Open activities. When transferring leads to a queue, open activities aren't transferred. |

When transferring accounts and their related data in Professional, Enterprise, Unlimited, Performance, and Developer Editions, all previous access granted by manual sharing, Apex managed sharing, or sharing rules is removed. New sharing rules are then applied to the data based on the new owner. To grant access to certain users, the new owner must manually share the transferred accounts and opportunities as necessary.

SEE ALSO:

[Transfer Records](#)

Delete Multiple Records and Reports

You can delete multiple reports or records at the same time.

The record types you can mass-delete include cases, solutions, accounts, contacts, leads, products, and activities.

Here are some ways that mass delete is handy.

- You've identified multiple reports that are no longer used and you want to unclutter the list of reports on the Reports tab.
- You imported your leads incorrectly and you want to start over.
- A user who recently left your company had contacts that were duplicates of other users' data and you want to delete these duplicate contacts.
- You used to enter leads as accounts with the `Type` field set to Prospect. You now want to convert these accounts into leads.

 **Tip:** Run a report of these accounts, export it to Excel, and then use the Import Leads wizard to import the data as leads. Then using mass delete, select accounts as the record type to delete and enter *Type equals Prospect* to locate all accounts you want to delete.

- You want to delete all the leads that have been converted for your org. Select the lead record type, enter *Converted equals 1* for the search criteria, and then click **Search**.
- You want to clean up web-generated leads that were created incorrectly or delete accounts and contacts with whom you no longer do business.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions**

This feature is only available in **Database.com** via the API. You can only mass delete records of custom objects in **Database.com**.

USER PERMISSIONS

To mass delete data:

- **Modify All Data**

1. We strongly suggest you run a report to archive your information and export your data weekly. See [Export Backup Data from Salesforce](#) on page 722.
2. From Setup, enter *Mass Delete Records* in the **Quick Find** box, then select **Mass Delete Records** and click the link for the type of record to delete.
3. Review the information that is deleted with the records.
4. Specify conditions that the selected items must match, for example, "State equals California."
5. If you're deleting accounts, specify whether you want to delete accounts with attached closed/won opportunities or attached opportunities owned by others.
6. If you're deleting products, select **Archive Products** if you also want to delete products that are on opportunities. This option deletes products that are not on opportunities and moves them to the Recycle Bin. It also archives products that are on opportunities. These products are not moved to the Recycle Bin and cannot be recovered.

To delete only those products that are not on opportunities, don't select **Archive Products**. Selected products that are on opportunities remain checked after the deletion to indicate that they were not included in the deletion.
7. To find records that match, click **Search** and select the items you want to delete. To select all currently displayed items, check the box in the column header.
8. To permanently delete records, select **Permanently delete the selected records**.

 **Important:** Selecting this option prevents you from recovering the selected records from the Recycle Bin.
9. Click **Delete**.
If you did not select **Permanently delete the selected records**, deleted items are moved to the Recycle Bin.

SEE ALSO:

[Notes on Using Mass Delete](#)[Undoing an Import](#)[Using Mass Delete to Undo Imports](#)

Notes on Using Mass Delete

Consider the following when using mass delete:

General Notes About Mass-Deleting

- You can delete up to 250 items at one time.
- When you delete a record, any associated records that display on that record's related lists are also deleted.
- Only reports in public report folders can be mass-deleted.
- You can't mass-delete reports that are attached to dashboards, scheduled, or used in reporting snapshots.

Notes About Mass Delete for Sales Teams

- You can't delete partner accounts that have partner users.
- Products on opportunities cannot be deleted, but they can be archived.
- When you mass-delete products, all related price book entries are deleted with the deleted products.
- When you delete activities, any archived activities that meet the conditions are also deleted.
- When you delete activities, requested meetings aren't included in the mass-delete until they are confirmed and automatically converted to events.
- When you delete recurring events, their child events are not displayed in the list of possible items to delete, but they are deleted.

Notes About Mass Delete for Service Teams

- Accounts and contacts associated with cases cannot be deleted.
- Contacts enabled for Self-Service, and their associated accounts, cannot be deleted.
- Deleting a master solution does not delete the translated solutions associated with it. Instead, each translated solution becomes a master solution.
- Deleting a translated solution removes the association with its master solution.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: **All Editions**

This feature is only available in **Database.com** via the API. You can only mass delete records of custom objects in **Database.com**.

USER PERMISSIONS

To mass delete data:

- **Modify All Data**

Mass Update Addresses

When your data is consistent, your reports and related metrics are more accurate and easier to understand. For example, having different abbreviations for a country/territory or state can skew your data. To make your addresses consistent, you can update country/territory and state/province information in existing fields at one time.

You can mass update addresses in contacts, contracts, and leads.

 **Tip:** To ensure data consistency in new records, consider using state and country/territory picklists. Mass Update works with standard address fields, but doesn't change Custom Address Fields.

1. From Setup, enter *Mass Update Addresses* in the **Quick Find** box, then select **Mass Update Addresses**.
2. Select **Countries** or **State/Province**. If you chose State/Province, enter the country or territory in which to update the state or province.
3. Click **Next**.
4. Select the values to update and click **Add**.

The Selected Values box displays the values to update.

The Available Values box displays the address values found in existing records. To find more addresses to update, enter all or part of a value and click **Find**.

If your organization has large amounts of data, instead of using the Available Values box, enter existing values to update in the text area. Separate each value with a new line.

5. In the **Replace selected values with** field, enter the value with which to replace the specified address data, and click **Next**. If your organization has large amounts of data, this field is called **Replace entered values with**.

The number and type of address records to update are displayed. If you have large amounts of data, only the values to update are displayed.

6. To update the values, click **Replace**.

SEE ALSO:

[Let Users Select States, Countries, and Territories from Picklists](#)

[Tips for Mass Updating Addresses](#)

Tips for Mass Updating Addresses

To save time and ensure that your filter settings are up-to-date, use these tips when you mass update country/territory and state/province information in existing address fields.

- Update countries and territories first, and then update states or provinces within that newly standardized country or territory value.
- Use the mass updating address tool to convert inconsistent address formats to one international standard, such as ISO codes. For a list of ISO codes, see the [International Organization for Standardization](#) website.
- Use the mass updating tool regularly to cleanse your address data of inconsistent values created by users or via import, sync, or the Lightning Platform API.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **All Editions** except for **Database.com**.

USER PERMISSIONS

To mass update addresses:

- Modify All Data

To mass update addresses of contracts:

- Modify All Data

AND

Activate Contracts

EDITIONS

Available in: Salesforce Classic (**not available in all orgs**)

Available in: **All Editions** except for **Database.com**.

- You can manually create any country/territory or state/province value or import or sync via the Lightning Platform API. Address values are not validated when created.
- Update filter conditions to reflect address updates. For example, if you change “United States” to “US,” assignment rules, Web-to-Lead, Web-to-Case, Email-to-Case, and On-Demand Email-to-Case continue to use “United States” unless updated.

SEE ALSO:

[Mass Update Addresses](#)

Scalability FAQ

Find answers to frequently asked questions about scalability.

- [How scalable is Salesforce?](#)
- [Do I see a degradation in performance as Salesforce's subscriber base grows?](#)

How scalable is Salesforce?

The service has the capacity to scale to the largest of teams. The architecture behind the service was designed to handle millions of users. We scale as rapidly as our customers require.

Do I see a degradation in performance as Salesforce's subscriber base grows?

No. We are very conscious of performance and have designed the service to be scalable in such a way that we can constantly stay ahead of customer demand. Our architecture lets us easily add web and application servers to accommodate more users. The system architecture also lets us add more database servers as needed to accommodate more users. In addition, the facility that houses our servers provides us with guaranteed bandwidth, which we can increase as needed.

Back Up Metadata to Protect and Restore Your Customizations

Protect your org’s customizations, such as custom fields, custom Apex code, page layouts, reports, and permission sets, by backing up your metadata.

Back Up Your Metadata

Backing up your metadata gives you a snapshot of that metadata at a particular point in time. At a future time, you can compare the backed-up metadata with more recent metadata. You might do this to revert your metadata to a previous state or to identify what changes have been made for purposes such as debugging.

To back up your metadata, create an unmanaged package.

1. In Setup, enter *Package Manager* in the Quick Find box, and then select **Package Manager**.
2. Select **New**, name the package, and select **Save**.
3. In the Components tab, select **Add**.
4. In the Component Type dropdown list, select the types of metadata you want to include in your backup, and click **Add To Package** for each metadata type.

EDITIONS

Available in: **Developer, Enterprise, Performance, Professional, and Unlimited** editions.

USER PERMISSIONS

To create unmanaged packages:

- Create AppExchange Packages and Manage Users

5. To finish creating this unmanaged package, click **Upload**.

You receive an email when your package has been uploaded to the Package Manager page.

 **Note:** Unmanaged packages don't support all metadata types. See [Components Available in Unmanaged Packages](#).

For more advanced metadata backup options, API and CLI commands are available. See [Deploying and Retrieving Metadata](#) in the *Metadata API Developer Guide* and [mdapi Commands](#) in the *Salesforce CLI Command Reference*. To review the metadata types that can be packaged using more advanced developer tools, see the [Metadata Coverage Report](#).

Create a New Version of Your Unmanaged Package

It's likely that your org's metadata is changing daily, and that new metadata types are added. To protect these changes, periodically create a new version of your unmanaged package.

Create a new version of your unmanaged package.

1. In Setup, enter *Package Manager* in the Quick Find Box, and then select **Package Manager**.
2. Click the Package Name for the unmanaged package you created.
3. In the Components tab, select **Add**.
4. In the Component Type dropdown list, select any new types of metadata you want to add to your backup, and click **Add To Package** for each metadata type.

 **Note:** Changes to components that were added in a previous package version are captured automatically when you create a new version.

5. Click **Upload**, and in the Package Detail screen complete the Version Name field. Consider adding details in the Description field so you know when this version was created, and click **Upload**.

Each time you create a new package version, you've created a new snapshot of your metadata.

Restore Your Metadata From an Unmanaged Package

We recommend restoring metadata in a sandbox org. Then use your standard method for deployment from a sandbox to your production org.

To restore your metadata from an unmanaged package:

1. In Setup, enter *Package Manager* in the Quick Find Box, and then select **Package Manager**.
2. Click the Package Name for the unmanaged package you created.
3. From the Package Detail page, click the Versions tab, and select the package version number.
4. Copy the installation URL from the Package Version Detail page.
5. Use the installation URL to install your unmanaged package in a sandbox org.
6. Work with a developer to retrieve and redeploy the metadata to restore using either the [Metadata API](#) or the [Salesforce CLI](#).

 **Note:** Third-party release management apps that automate data and metadata backup are available on AppExchange.

SEE ALSO:

[Trailhead: Package Development Readiness](#)

[Trailhead: Package Development Model](#)

Protect Your Data with Salesforce Backup

Use Salesforce Backup to prevent data loss, recover from data incidents quickly, and simplify your overall data management strategy. Protect your organization from permanent data loss and corruption by automatically generating backups. You can create backup policies for high-value and regulated data, and restore that data in just a few clicks.

1. [Assign the Permission Set License for Salesforce Backup](#)

The Backup and Restore Permission Set License gives users the required permissions to install and use the Salesforce Backup managed package.

2. [Assign Salesforce Backup Permissions](#)

Give users access to the Salesforce Backup app. Then assign them permission to back up and restore data on specific objects.

3. [Install and Set Up the Salesforce Backup Managed Package](#)

Salesforce Backup is a managed package that you install. After you assign the necessary license and permissions, install the package using the link from your subscription order form. Then configure a secure connection between the app and Salesforce.

4. [Plan Your Salesforce Backup Strategy](#)

To create high-value and time-efficient policies, make a plan for identifying and prioritizing the data that you want to back up. Then make sure that users have access to the objects that store data and build your backup policy in batches.

5. [Create a Backup Policy](#)

When you're ready to start backing up data with the Salesforce Backup app, create and activate your policy. Backups occur once every 24 hours starting at 6:00 PM Central Time (GMT - 6).

6. [Restore Data from a Backup](#)

The Salesforce Backup app can restore your data from a backup for you. You can also export data from a backup and restore it with a data import tool such as Data Loader or Data Import Wizard. Before you start, make sure that you have object-level permissions for the records that you want to restore.

7. [View and Interpret Salesforce Backup Logs](#)

Follow these instructions to view logs in Salesforce Backup. These logs contain information about the status of various Salesforce Backup policies and activity.

8. [Troubleshoot Salesforce Backup](#)

Salesforce Backup shows status codes for specific errors that can happen during backup and restore processes. Use this guide to determine what an error code indicates and how to fix the problem.

9. [Salesforce Backup Considerations](#)

Before using Salesforce Backup, review these considerations.

EDITIONS

Available in: **Lightning Experience**

Available in: **Professional, Enterprise, Performance, and Unlimited** Editions

Requires the Backup and Restore add-on subscription.

Assign the Permission Set License for Salesforce Backup

The Backup and Restore Permission Set License gives users the required permissions to install and use the Salesforce Backup managed package.

Each Salesforce Backup user needs the Salesforce Backup User Permission Set License and the BackupRestore Permission Set.

1. From Setup, in the Quick Find Box, enter `users`, and then select **Users**. Select the users that you want to grant access to Salesforce Backup.
2. From Permission Set License Assignments, click **Edit Assignments**, and select **Backup and Restore User Permission Set License**.
3. Save your work.

You can now assign the BackupRestore permission set to users. Backup and restore processes depend on the user's object permissions. Before adding objects to a backup policy, review which object permissions different actions require.

Assign Salesforce Backup Permissions

Give users access to the Salesforce Backup app. Then assign them permission to back up and restore data on specific objects.

Salesforce Backup requires access to Salesforce data when creating copies of data for backup and when updating or creating records during restore operations. Configure the permissions of the individual user who initiates backup and restore operations. Also configure permissions for the Integration User.

1. From Setup, in the Quick Find Box, enter `users`, and then select **Users**. Select the users that you want to grant access to Salesforce Backup.
2. From Permission Set Assignments, click **Edit Assignments**.
3. Under Available Permission Sets, select **BackupRestore**, click **Add**, and then save your work. You can now assign object permissions to users.
4. Give users access to the objects they plan to manage in Salesforce Backup.
 - [Edit object permissions in profiles](#).
 - [Create a permission set](#) with the relevant object-level permissions and assign it to users.

Use this reference table to match the correct object permission for different backup and restore tasks.

| User Task | Object Permission |
|-------------------------------|------------------------|
| Back up records | Read |
| Restore records | Read, create, and edit |
| Restore only existing records | Edit |
| Restore only deleted records | Create |

EDITIONS

Available in: Lightning Experience

Available in: **Professional, Enterprise, Performance,** and **Unlimited** Editions

Requires the Backup and Restore add-on subscription.

USER PERMISSIONS

To assign a permission set license:

- [Manage Users](#)

EDITIONS

Available in: Lightning Experience

Available in: **Professional, Enterprise, Performance,** and **Unlimited** Editions

Requires the Backup and Restore add-on subscription.

USER PERMISSIONS

To assign permission sets:

- [Assign Permission Sets](#)
- AND

[View Setup and Configuration](#)

To edit object permissions:

- [Manage Profiles and Permission Sets](#)
- AND

[Customize Application](#)

[Customize Application](#)

Install and Set Up the Salesforce Backup Managed Package

Salesforce Backup is a managed package that you install. After you assign the necessary license and permissions, install the package using the link from your subscription order form. Then configure a secure connection between the app and Salesforce.

User Permissions Needed

| | |
|---|----------------------|
| To install the Salesforce Backup managed package: | Modify All Data |
| | AND |
| | System Administrator |

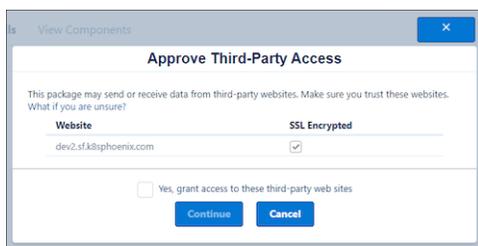
EDITIONS

Available in: Lightning Experience

Available in: **Professional, Enterprise, Performance,** and **Unlimited** Editions

Requires the Backup and Restore add-on subscription.

1. Find the order form that your organization received when you purchased Backup and Restore. It contains the installation URL.
2. Click the URL, and then download the Salesforce Backup managed package.
3. From the Managed Package page, select **Install for Admins Only**. If you're prompted to approve third-party access, select **Yes, grant access to these third-party web sites**, and then click **Continue**. Although `dev2.sf.k8phoenix.com` isn't a third-party URL, Salesforce uses this domain to support the backup and restore process.



You receive an email notification that the package is installed.

4. Assign yourself the Salesforce Backup User permission set license and BackupRestore permission set. See [Assign the Permission Set License for Salesforce Backup](#) and [Assign Salesforce Backup Permissions](#).
5. In the Salesforce Backup app, click the **Settings** tab.
6. In the Provision a Region section, from the dropdown menu, select the AWS region where you want to store your backups. When choosing a region, keep in mind any data residency requirements that apply to your organization.
7. If you have no IP restrictions, click **Start**. However, if you do have IP restrictions:
 - a. Add the IP address for the Salesforce Backup provisioning API (3.219.91.219) to the [Login IP Ranges](#) on your profile, and then click **Start**.
When provisioning is finished, an IP Addresses section appears on the page. It lists IP addresses that are specific to the AWS region that you selected.
 - b. Add the IP addresses in the IP Addresses section to the Login IP Ranges for your user profile.
8. In the Set Up Your Connection section, click **Connect**. This action creates a secure connection using OAuth 2.0 Web Server Flow between Salesforce and the data storage location in AWS.
9. Click **Test Connection**.
When the test is successful, you're ready to create a backup policy.

Plan Your Salesforce Backup Strategy

To create high-value and time-efficient policies, make a plan for identifying and prioritizing the data that you want to back up. Then make sure that users have access to the objects that store data and build your backup policy in batches.

Follow these tips to make the most of your team's time, increase your successful backup rate, and spend less time fine-tuning your backup policy.

Identify and Prioritize the Data That You Want to Back Up

Most customers have specific goals for backing up data. Some customers want to keep backups for security purposes, while others aim to meet compliance requirements for certain categories of data, such as health data. Whatever your goals, it's important to know what information is most important to your security and compliance posture.

Talk with your team to identify high, medium, and low-priority data for backup. Then identify and list the objects that contain that data.

Give Authorized Users Access to Object

The Salesforce Backup application respects object access rules and only acts on objects that you have access to. Without full object access, backups don't complete or aren't available for restoration later. Most backup and restore issues stem from incorrect object access settings.

After you have a prioritized list of objects, make sure that integration users have access to them.

- Assign read access to all objects that you plan to back up.
- Ensure that you meet all special access rules. For example, some objects are only available in specific products or when features within those products are enabled. Review the Special Access Rules section of the object reference documentation for the licenses, permissions, and preferences that each object requires.
- Custom objects, including custom objects in managed packages, must be available site-wide.

Users must have all levels of access before an object can be backed up. See the Special Access section on each object's entry in the [Object Reference for the Salesforce Platform](#) guide.

To confirm and modify object access, use the Object Manager and Profile pages in Setup along with the User Licenses related list on the Company Information page.

Follow Up After You Restore Data

As you plan what data to back up, it's a good idea to set aside time to review the data after you restore it. Evaluating restored data not only helps you validate your backup strategy, but it also helps you stay on top of important data cleansing and maintenance tasks.

For example, you can back up and restore share object data. If you changed your share settings between the time that a share object was backed up and restored, restoring that share object can introduce unwanted object access settings. After you restore share objects, revisit those objects' manual sharing settings or Apex share settings and verify that they adhere to your current object access policies.

EDITIONS

Available in: Lightning Experience

Available in: **Professional, Enterprise, Performance,** and **Unlimited** Editions

Requires the Backup and Restore add-on subscription.

Create a Backup Policy

When you're ready to start backing up data with the Salesforce Backup app, create and activate your policy. Backups occur once every 24 hours starting at 6:00 PM Central Time (GMT - 6).

In addition to object permissions, you must meet all special access rules for each object that you add to a policy. For example, some objects are only available in specific products, when features within those products are enabled, or with product-specific permission sets. Review the Special Access Rules section of the object reference documentation for all required licenses, permissions, and preferences.

1. From the App Launcher, find and select **Backup and Restore**.
2. To create a backup policy, from the Backup tab, click **Create Policy**.
3. Select an object from the list.
A list of related objects appears.
4. Select any related objects that you want to add to your policy, and click **Save Related Objects**.
5. To add your selected objects to your policy, select **Enable**.
Objects in your policy show as enabled and ready in the object list.
6. Continue adding objects and their related objects to your policy.
7. When your policy contains all of the data that you want to back up, click **Activate Policy**.
When activated, backup policies run once every 24 hours. Monitor your backup job on the Home or Logs pages.

EDITIONS

Available in: Lightning Experience

Available in: **Professional, Enterprise, Performance, and Unlimited** Editions

Requires the Backup and Restore add-on subscription.

USER PERMISSIONS

To back up objects:

- Read on each object

To edit object permissions:

- Manage Profiles and Permission Sets

AND

Customize Application

Restore Data from a Backup

The Salesforce Backup app can restore your data from a backup for you. You can also export data from a backup and restore it with a data import tool such as Data Loader or Data Import Wizard. Before you start, make sure that you have object-level permissions for the records that you want to restore.

In addition, you must meet all special access rules for each object that you add to your policy. For example, some objects are only available in specific products, when features within those products are enabled, or with product-specific permission sets. Review the Special Access Rules section of the object reference documentation for all required licenses, permissions, and preferences.

1. From the Restore tab, set your record filters. Select the object that you want to restore records on, the date of the backup that you want to restore, and the type of change in the record.

2. Click **Show Records**.

A list of all objects that meet your criteria appears. When lookup relationship fields share data across objects, related records are nested under parent records. Lookup field IDs are shown to help you see how restored data propagates across your implementation.

3. Select a record.

4. To compare the latest version of records on an object against your chosen backup, on a record row, click the Actions dropdown (☰), and then select **Compare**.

5. Click **Next**.

The page refreshes with related objects and record version options.

6. Select a related object that you want to add to your restore job.

7. Choose the backup version that you want to restore updated and deleted objects to on that record.

- Choose backup versions on a record-by-record basis.
- To bulk update all records of a specific change type, choose a default action, and then click **Apply Defaults**.

8. Choose a restoration method.

- To restore data directly from the Salesforce Backup app, click **Restore**. In the window that opens, confirm your selections. Use this method for most restoration jobs.
- To restore data with another tool, click **Export**. In the window that opens, confirm the download. When the download finishes, import the data with a tool such as Data Loader or the Data Import Wizard. Use this method if a schema change, such as a new or deleted field, prevents a record from being automatically restored.

Restoration jobs completed by the Salesforce Backup app normally finish within 10 minutes. The user who initiates a restoration job receives an email when the process finishes. Exported CSV files save to your Downloads folder. Larger files take longer to download. Review restore and export statuses on the Logs tab.

 **Tip:** Some macOS X versions can't decompress and open the downloaded CSV file. If you can't open the downloaded file, try running the `gunzip '/path/to/your_file.csv'` command in a terminal. Alternatively, you can use another data decompression utility.

EDITIONS

Available in: Lightning Experience

Available in: **Professional, Enterprise, Performance, and Unlimited** Editions

Requires the Backup and Restore add-on subscription.

USER PERMISSIONS

To restore records on all objects:

- Read, Create, and Edit on each object

To restore only existing records on objects:

- Edit on each object

To restore only deleted records on object:

- Create on each object

To edit object permissions:

- Manage Profiles and Permission Sets

AND

Customize Application

View and Interpret Salesforce Backup Logs

Follow these instructions to view logs in Salesforce Backup. These logs contain information about the status of various Salesforce Backup policies and activity.

1. Click the Logs tab. You can review the time a job began and its status.
2. To see details about a backup or restore job, in the Log Name column, click an entry.
3. On the log detail page, review information about the job, including when it finished, the Run ID, its status, and the objects included in the backup or restore job.
 - For a list of all objects included in the job, select the All Objects tab.
 - If a job completed with errors, select the Objects with Errors tab. Use the Object Status column to identify the cause of the error.

Logs display the status of the backup for each object. If a backup is incomplete, you can review the logs to see errors on specific objects.

The NOT_VISIBLE status in the backup log indicates that an object isn't visible to the service at the time that the backup process ran and it hasn't been backed up. When the service can't back up an object, the most common issue is that the user running the backup doesn't meet one or more of the required access conditions. Review all access settings for objects that show the NOT_VISIBLE status in logs. Correct any access gaps, then run the backup again.

- The user doesn't have the required object-level permissions, such as read permission.
- The user initiating the backup, including automated users like Integration User, didn't have the required licenses and permission sets.
- Not all special access rules for the object are met.
- The user has access to a custom object, but it's in a managed package that isn't site-wide.

Troubleshoot Salesforce Backup

Salesforce Backup shows status codes for specific errors that can happen during backup and restore processes. Use this guide to determine what an error code indicates and how to fix the problem.

If a backup or restore process ends with an error, status codes on the Log Detail page indicate the cause of the error. Use this table to identify causes and solutions to the most likely issues. If your process ends in an error that's not listed here, contact Salesforce Customer Support for help.

Table 5: Salesforce Backup Error Status Codes

| Status Code | Error Cause | Tips for Fixing the Problem |
|-----------------------|--|--|
| DUPLICATE_EXTERNAL_ID | A user-specified external ID matches more than one record. | Export to CSV and manually edit the values as needed before importing your data. |
| ENTITY_IS_DELETED | The backup or restore job references an object that's been deleted. If you try to restore a child record when the parent record is deleted, this error message appears because the child ID value doesn't exist. | Restore the parent and child record, so the child ID is recreated and updated. |

EDITIONS

Available in: Lightning Experience

Available in: **Professional, Enterprise, Performance, and Unlimited** Editions

Requires the Backup and Restore add-on subscription.

EDITIONS

Available in: Lightning Experience

Available in: **Professional, Enterprise, Performance, and Unlimited** Editions

Requires the Backup and Restore add-on subscription.

| Status Code | Error Cause | Tips for Fixing the Problem |
|---|---|---|
| ENTITY_IS_LOCKED | An approval process has locked a record, rendering it read-only. | To restore the record, you must have record-level edit access. Ask an admin to temporarily disable the approval process. When the restoration job is done, they can reinstate the approval process. |
| FIELD_CUSTOM_VALIDATION_EXCEPTION | A custom validation formula in the backup or restore job violates a field integrity rule. | Update the field integrity rule to allow the value to be restored. You can also export the backup as a CSV and manually edit the values as needed before importing your data. |
| FIELD_FILTER_VALIDATION_EXCEPTION | One or more fields in the backup or restore job violate field integrity rules. | Update the rule to allow the value to be restored. You can also export to CSV and manually edit the values as needed before importing your data. |
| INACTIVE_OWNER_OR_USER | An inactive user owns one or more records in the backup or restore job. | Reactivate the inactive user or reassign record ownership to an active user. You can also export to CSV and manually edit the values as needed before importing your data. |
| INVALID_OR_NULL_FOR_RESTRICTED_PICKLIST | Either the restore job includes a picklist whose values are restricted to a defined set that doesn't match the backup or the backup contains one or more null values. | Adjust the picklist values to match the values present in the backup, and then run the restore job. You can also export to CSV and manually edit the values as needed before importing your data. |
| INVALID_SESSION_ID | Either the specified session ID is malformed, such as with an incorrect length or format or the session has expired. | Reconnect the app's connection on the Settings tab or log in again to start a new session. |
| INVALID_TYPE_ON_FIELD_IN_RECORD | The field value on the record isn't valid for the field's type. Invalid record types can happen when the object's schema has changed and is no longer compatible with the backed-up data. | Export to CSV and manually edit the values as needed before importing your data. |
| INVALID_USERID | The backup or restore process references the user ID for a user that isn't an active member of your org. | Export to CSV and manually edit the values as needed before importing your data. |
| INVALID_USER_OBJECT | The user object isn't valid. | Export to CSV and manually edit the values as needed before importing your data. |
| REQUIRED_FIELD_MISSING | A call requires a field that wasn't specified. | Recreate the missing field on the record and then run the restore job. You can also export to CSV and manually edit the values as needed before importing your data. |

| Status Code | Error Cause | Tips for Fixing the Problem |
|----------------------------------|--|---|
| SELF_REFERENCE_FROM_TRIGGER | <p>Apex triggers that recursively update or delete an object interfere with backup and restore jobs. Common causes of this error are when an object is updated or deleted from within a <code>before</code> trigger, or when an object is deleted from within an <code>after</code> trigger. This error occurs with both direct and indirect operations.</p> <p>For example, a request is submitted to update Object A. A <code>before update</code> trigger on object A creates a second object, object B. Object A is updated. An <code>after insert</code> trigger on object B then queries object A and updates it. This update is an indirect update on object A because of the <code>before trigger</code>. An error is generated.</p> | <p>Fix the Apex trigger code causing the issue. You can also export to CSV and manually edit the values as needed before importing your data.</p> |
| UNABLE_TO_LOCK_ROW | <p>A deadlock or timeout condition has been detected. A deadlock involves at least two transactions that update overlapping sets of objects. If the transaction involves a summary field, the parent objects are locked, making these transactions especially prone to deadlocks.</p> <p>A timeout occurs when a transaction takes too long to complete. The timeout state is temporary. No action is needed. However, if an object in a batch can't be locked, the entire batch fails with this error.</p> | <p>When available, these error messages contain the IDs of the records that couldn't be locked. Temporarily disable any workflows or automations that can interfere.</p> <p>You can also export to CSV and manually update the values as needed before importing your data.</p> |
| UNAVAILABLE_RECORDTYPE_EXCEPTION | <p>The required default record type couldn't be found.</p> | <p>Recreate the appropriate RecordType. You can also export to CSV and manually edit the values as needed before importing your data.</p> |
| UNKNOWN_EXCEPTION | <p>The system encountered an internal error.</p> | <p>Contact Salesforce Customer Support and provide your org ID, execution ID, and filter settings.</p> |

SEE ALSO:

[SOAP API Developer Guide: Core Data Types Used in API Calls](#)

Salesforce Backup Considerations

Before using Salesforce Backup, review these considerations.

Salesforce Backup doesn't support certain objects.

- Objects that [aren't supported by the Bulk API](#)
- Records stored in big objects
- Standard objects that don't contain the CreatedDate, LastModifiedDate, and SystemModstamp [system fields](#), and the LoginDate field. If you have all required permissions and access levels enabled for an object, but the backup log status shows NOT_VISIBLE, the object is likely missing one or more of these required fields.
- History objects aren't backed up because they can't be restored. History tables are read-only.

Keep these other considerations in mind.

- When a record is updated, the original record ID is maintained. Only the fields that were changed get restored.
- When a record is deleted, a new record ID is created to restore that record.
- If a custom object is part of a managed package that's not site-wide, integration users must have the license for the object.
- Backup and restore operations involve the integration user. If your backup policy includes fields encrypted with Classic Encryption, make sure that the integration user has the View Encrypted Data permission. Otherwise, those fields' contents aren't accessible to the backup service. Their data isn't backed up and may not be restored.

EDITIONS

Available in: Lightning Experience

Available in: **Professional, Enterprise, Performance, and Unlimited** Editions

Requires the Backup and Restore add-on subscription.

Cache Lightning Platform Data

Using the Platform Cache can enable applications to run faster because they can store reusable data in memory. Applications can quickly access this data, removing the need to duplicate calculations and requests to the database on subsequent transactions.

To use Platform Cache, first set up partitions using the Platform Cache Partition tool in Setup. Once you've set up partitions, you can add, access, and remove data from them using the Platform Cache Apex API.

Use Platform Cache partitions to improve the performance of your applications. Partitions allow you to distribute cache space in the way that works best for your applications. Caching data to designated partitions ensures that it's not overwritten by other applications or less-critical data.

To access the Partition tool in Setup, enter *Platform Cache* in the **Quick Find** box, then select **Platform Cache**.

Use the Platform Cache Partition tool to:

- Setup a Platform Cache partition with Provider Free capacity.
- Request trial cache.
- Create, edit, or delete cache partitions.
- Allocate the session cache and org cache capacities of each partition to balance performance across apps.
- View a snapshot of the org's current cache capacity, breakdown, and partition allocations (in KB or MB).
- View details about each partition.
- Make any partition the default partition.

To use Platform Cache, create at least one partition. Each partition has one session cache and one org cache segment and you can allocate separate capacity to each segment. Session cache can be used to store data for individual user sessions, and org cache is for data that any users in an org can access. You can distribute your org's cache space across any number of partitions. Session and org cache allocations can be zero, or five or greater, and they must be whole numbers. The sum of all partition allocations, including the

default partition, equals the Platform Cache total allocation. The total allocated capacity of all cache segments must be less than or equal to the org's overall capacity.

You can define any partition as the default partition, but you can have only one default partition. When a partition has no allocation, cache operations (such as get and put) are not invoked, and no error is returned.

Capacity calculations occur every 5 minutes by default. To make sure you're seeing the latest capacity and allocation, click **Recalculate**.

[Request a Platform Cache Trial](#)

To test performance improvements by using Platform Cache in your own org, you can request trial cache for your production org. Enterprise, Unlimited, and Performance editions come with some cache, but adding more cache often provides greater performance. When your trial request is approved, you can allocate capacity to partitions and experiment with using the cache for different scenarios. Testing the cache on a trial basis lets you make an informed decision about whether to purchase cache.

[Request Additional Platform Cache](#)

You can request additional Platform Cache space to improve the performance of your application.

[Set Up a Platform Cache Partition with Provider Free Capacity](#)

Salesforce provides 3 MB of free Platform Cache capacity for security-reviewed managed packages. This is made available through a capacity type called Provider Free capacity and is automatically enabled in all Developer edition orgs.

SEE ALSO:

[Apex Developer Guide](#)

Request a Platform Cache Trial

To test performance improvements by using Platform Cache in your own org, you can request trial cache for your production org. Enterprise, Unlimited, and Performance editions come with some cache, but adding more cache often provides greater performance. When your trial request is approved, you can allocate capacity to partitions and experiment with using the cache for different scenarios. Testing the cache on a trial basis lets you make an informed decision about whether to purchase cache.

Salesforce approves trial cache requests immediately and sends you an email to notify you that your Platform Cache trial is active. It can take a few minutes for you to receive the email. You receive 30 MB of trial cache space (10 MB if you have Developer Edition). If you need more trial cache space, contact Salesforce.

 **Note:** You can make up to 10 trial cache requests, and you must wait 90 days between trials.

After you request trial cache, you receive emails at the following intervals.

At activation

You can now allocate capacity to partitions and test the trial cache in your org.

Three days before expiration

Before expiration, be sure to reconfigure your partitions to deallocate the added trial space.

At expiration

The trial cache is removed from your org.

 **Note:** If you haven't deallocated enough space, Salesforce reduces your partition sizes to remove the granted trial cache space.

Developer Edition Orgs

You can request trial cache for a Developer Edition org. After you sign up for the org, request trial cache from the Platform Cache Partition tool. ISVs who are using Developer Edition orgs to create managed packages can get 10 MB of trial cache for up to two Developer Edition orgs. ISVs can contact their Salesforce representative to get trial cache in Developer Edition orgs.

Cache Reduction Algorithm

At the end of your trial period, Salesforce removes the granted trial cache space from your org. Before your trial ends, make sure that you've deallocated your trial cache space. You can deallocate space from the Platform Cache Partition tool by resetting partition allocations. If you don't deallocate the cache space, Salesforce removes the granted cache using the following process.

- The system removes cache from the smallest non-default partition first.
 -  **Note:** The size of a partition is the total allocation for the partition, which includes org-wide cache and namespace-specific cache.
- The system then works its way through the partitions from smallest to largest in size. If multiple partitions have the same size, the system proportionally removes cache from these partitions.
- The system reduces partitions to a minimum size of 5 MB, unless all the trial cache space can't be removed. In this case, partitions are reduced to 0 MB.
- The default partition (if it exists) is reduced last only if the trial cache space can't be removed from all other partitions.

If unallocated space is present:

- If the amount of unallocated space is greater than the amount of space that must be removed, the system removes only unallocated space.
- If the amount of unallocated space is less than the amount of space that must be removed, the system removes the unallocated space first. The system then follows the cache reduction process to remove the remaining amount.

SEE ALSO:

[Cache Lightning Platform Data](#)

Request Additional Platform Cache

You can request additional Platform Cache space to improve the performance of your application.

Platform Cache is available to customers with Enterprise Edition orgs and above. The following editions come with some default cache space, but often, adding more cache gives even greater performance enhancements.

- Enterprise Edition (10 MB by default)
- Unlimited Edition (30 MB by default)
- Performance Edition (30 MB by default)

To determine how much cache would be beneficial to your applications, you can request trial cache and try it out in your org. Platform Cache can improve performance in the following situations, among many others.

- Orgs with a large amount of Apex customization
- Orgs with large numbers of concurrent users
- Orgs or applications with complex calculations or queries

In addition, ISVs can request additional cache for use with the applications they provide to customers.

Cache space is available in 10-MB blocks, with an annual subscription. To request additional Platform Cache, contact your Salesforce representative.

SEE ALSO:

[Cache Lightning Platform Data](#)

Set Up a Platform Cache Partition with Provider Free Capacity

Salesforce provides 3 MB of free Platform Cache capacity for security-reviewed managed packages. This is made available through a capacity type called Provider Free capacity and is automatically enabled in all Developer edition orgs.

Follow the steps here to allocate the Provider Free capacity to a Platform Cache partition before adding it to your managed package.

 **Note:** If a Platform Cache partition is already part of your managed package, you can choose to edit the existing partition and allocate the Provider Free capacity to it.

Create a partition from the Platform Cache page and then set it up to use the Provider Free capacity

1. From Setup, in the Quick Find box, enter *Platform Cache*, and then select **Platform Cache**.

As the Provider Free capacity is automatically enabled in all Developer edition orgs, the Org's Capacity Breakdown donut chart shows the Provider Free capacity.

2. Click **New Platform Cache Partition**.
3. In the `Label` box, enter a name for the partition. The name can contain alphanumeric characters only and must be unique in your org.
4. In the `Description` box, enter an optional description for the partition.
5. In the Capacity section, allocate separate capacities for session cache and org cache from the available Provider Free capacity.
6. Save the new Platform Cache partition.

You can add this new Platform Cache partition to your managed package. When a security-reviewed managed package with Platform Cache partition is installed on the subscriber org, the Provider Free capacity is allocated and automatically made available to the installed partition. The managed package can start using the Platform Cache partition; no post-install script or manual allocation is required.

 **Note:** If the managed package is not AppExchange-certified and security-reviewed, the Provider Free capacity resets to zero and will not be allocated to the installed Platform Cache partition.

When a Platform Cache partition with Provider Free capacity is installed in a subscriber org, the Provider Free capacity allocated is non-editable. The provider free capacity of one installed partition can't be used for any other partition.

 **Tip:** After you install a Platform Cache partition with Provider Free capacity, you can edit the partition and make additional allocations from the available platform cache capacity of the org.

SEE ALSO:

[Cache Lightning Platform Data](#)

My Domain

Showcase your company's brand with a customer-specific subdomain name in your Salesforce org URLs. With My Domain, you can include your company name in your URLs, for example, `https://mycompany.my.salesforce.com`. With these org-specific URLs, you can set up a custom login page, set a custom login policy, offer single sign-on, and allow users to log in with a social account. My Domain also allows you to work in multiple Salesforce orgs in the same browser at the same time.

All orgs get a My Domain with enhanced domains by default. If you don't like your org's My Domain name or circumstances warrant a change, you can rename it.

 **Note:** A My Domain uses Salesforce domain suffixes such as `my.salesforce.com` for your org's URLs. With enhanced domains, your My Domain name is also used in the system-managed hostnames for your Salesforce Sites and Experience Cloud sites URLs. To use a custom domain such as `https://www.example.com` to serve your org's Salesforce Sites and Experience Cloud sites, see [Custom Domains](#) in Salesforce Help.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

Brand Your Salesforce Org's Domains

Understand how to include your brand in the URLs used to access your Salesforce org and its data with My Domain, Experience Cloud sites, Salesforce Sites, and custom domains.

What Is My Domain?

Showcase your company's brand with your My Domain name. That My Domain name is used as your org-specific subdomain in Salesforce login and application URLs. For example, `https://mycompany.my.salesforce.com` and `https://mycompany.my.site.com`. Learn about the benefits of My Domain, including a custom login page and user login and authentication options.

My Domain Considerations

When you deploy a change to your My Domain, it's important to understand the impact on URLs across your Salesforce org. Review these considerations about URL changes, feature testing, and reducing the impact to your users.

My Domain Provisioning and Deployment

Understand the provisioning and deployment process when you rename your My Domain name, change your My Domain suffix, or enable enhanced domains. Learn about how each step of the process impacts your user's access to Salesforce and why it's important to test these changes in a sandbox.

Enhanced Domains

Enhanced domains are the current version of My Domain that meets the latest browser requirements. With enhanced domains, all URLs across your org contain your company-specific My Domain name, including URLs for your Experience Cloud sites, Salesforce Sites, Visualforce pages, and content files. This feature changed domain suffixes (the part after the My Domain name) to meet the latest security standards. With no instance names, enhanced My Domain URLs are easier for users to remember and don't change when your org is moved to another Salesforce instance. Because enhanced domains meet the latest browser requirements, this feature was enforced in Winter '24.

Partitioned Domains

With partitioned domains, My Domain hostnames for your Developer Edition org, demo org, patch org, sandbox, scratch org, or Trailhead Playground include a word related to the org type. For example, partitioned domains for Developer Edition and patch orgs include the word `develop`. Partitioned domains allow Salesforce to maximize the availability of your orgs by gradually rolling out delivery changes. And it's easier to identify an org by a URL when the domain is partitioned.

[Plan for a My Domain Change](#)

Whether you change your My Domain to update your brand, to adopt enhanced domains, or to enable partitioned domains, the URLs that Salesforce hosts for your org change. Those changes can have a large impact, and making the required updates can seem like a daunting project. To make the process as smooth as possible for you, your users, and your customers, review the high-level steps, the recommended practices, and how to reduce the impact on your users and customers.

[Change Your My Domain Details](#)

If you don't like your My Domain or circumstances warrant a change, you can rename it. For example, you can change the name when your company's name or branding changes. In some orgs, the admin can also choose a different domain suffix, enable enhanced domains, and remove instance names from certain My Domain URLs.

[Update Your Org and Test My Domain Changes](#)

Before you deploy a change to your My Domain, work with your users to preserve their login access to your org. To test My Domain changes, deploy the change in a sandbox. If your My Domain login URL or site URL changes, update authentication. Review and make the required updates to support the new domains. Then test access to your org and your functional workflows in Salesforce. After you complete testing in a sandbox, use the same process to update your production org. Finally, update redirection behavior for your old URLs.

[My Domain Redirections](#)

When you deploy a change to your My Domain, Salesforce redirects multiple hostnames automatically. Learn about the types of redirections, how to log redirections for the hostnames that Salesforce hosts for your org, and how you can control these redirections.

[Configure My Domain Settings](#)

Determine the user experience when logging into your Salesforce org via your My Domain. Manage user logins and authentication methods and customize your login page with your brand. Control whether users are redirected when they visit URLs that Salesforce previously served for your org.

[Salesforce Edge Network](#)

Users access your Salesforce data from all over the world. Salesforce Edge Network delivers a consistent user experience regardless of a user's location. It improves download times and the user's network experience. The move to Salesforce Edge Network is seamless for your users. They keep using the same URLs to access your org, only with a better experience.

[Get Your Org Status and Upcoming Maintenance Dates with My Domain](#)

Get information about system performance and availability from `trust.salesforce.com`. This trust page reports status information based on your Salesforce instance. If you don't know your instance, use your My Domain name to look it up.

[Link to Salesforce Domains in Packages](#)

If you provide a package to Salesforce customers through AppExchange, review your code for hard-coded URLs and code that parses a known URL. The URLs that Salesforce serves for a target org vary based on the org type and configuration. Hard-coded URLs and code that assumes the format of a URL can break when a customer enables enhanced domains, enables partitioned domains, or changes their My Domain name. Also, URL formats can vary between production orgs, sandboxes, and other non-production orgs. To ensure that your package functionality continues to work with all possible URL formats, update hard-coded URL references to relative URLs whenever possible. When a relative URL isn't possible, use a dynamically generated hostname.

[Log In to Salesforce with Code](#)

For an extra layer of security, use your My Domain login URL to access your Salesforce org with code. Compare the benefits of your My Domain login URL versus the default Salesforce login URL. And understand why we don't recommend that you use URLs that contain your Salesforce instance.

[My Domain URL Formats](#)

Your My Domain name is a subdomain used in login URL and application URLs across your Salesforce org, including sites and Visualforce pages. Understand what determines your org's URL formats and the structure of those formats.

SEE ALSO:

[Custom Domains](#)

Brand Your Salesforce Org's Domains

Understand how to include your brand in the URLs used to access your Salesforce org and its data with My Domain, Experience Cloud sites, Salesforce Sites, and custom domains.

Various users access your Salesforce org, each with their own needs.

- Sales representatives log in to the Salesforce application to view and manage their sales opportunities.
- Customers and partners log in to your Salesforce Experience Cloud sites to connect with your employees and each other.
- Public users log in to a Salesforce Site to access public data from your org, such as a recruiting website, store locator, or an ideas website.
- Consumers and businesses visit your storefronts to purchase products.
- External systems use API calls to access your org's data.
- Admins maintain your org and keep everything running smoothly.

Each of these interactions involves at least one URL, and those URLs are based on your Salesforce org's domains. Salesforce offers features that affect your org's URLs. Each option allows you to incorporate your brand into your URLs, making it easier for users and admins to remember them.

You also have the option to require that users and SOAP API calls use your My Domain login URL when accessing your org. Because your My Domain login URL is unique to your org, requiring API calls to use it adds an extra layer of security.

My Domain

My Domain allows you to showcase your company's brand with a customer-specific domain name within your Salesforce org login and application URLs. For example, if your org's My Domain name is *mycompany*, then your org's login URL is `https://mycompany.my.salesforce.com`. All orgs get a My Domain by default. If you don't like your org's My Domain name, you can change it.

If enhanced domains are enabled in your org, the My Domain name is used as the subdomain for URLs across your org, including Salesforce Sites and Experience Cloud sites.

If enhanced domains aren't enabled in your org, you specify separate subdomains for Experience Cloud sites and Salesforce Sites. One of these subdomains can match your My Domain name, but if you have Salesforce Sites and Experience Cloud sites, those subdomains can't be the same. You can rename your My Domain name, but you can't change your Experience Cloud sites subdomain or Salesforce Sites subdomain after you save them. Choose these subdomains carefully to ensure brand consistency. Or better yet, use enhanced domains, and your My Domain name is the subdomain for these features.

Experience Cloud Sites

Experience Cloud sites are a great way to share information and collaborate with customers, partners, and employees. Whether you call it a portal, a help forum, a support site, HR central, or something else, Experience Cloud sites provide an online community.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

If enhanced domains are enabled in your org, your My Domain is used as your Experience Cloud sites subdomain. The Experience Cloud sites URL format is `https://MyDomainName.my.site.com`.

If enhanced domains aren't enabled in your org, when you enable Experience Cloud Sites, you register an Experience Cloud sites domain for your org. Like with Salesforce Sites, you pick the subdomain name, and Salesforce adds the domain suffix. The suffix for Experience Cloud sites is `force.com`. For example, if you choose `mycompany-portal` as your Experience Cloud sites subdomain, your Experience Cloud sites domain is `https://mycompany-portal.force.com`. If you haven't used your My Domain name for your Salesforce Sites subdomain name, you can use your My Domain name as your Experience Cloud sites subdomain name. However, after you choose your Experience Cloud sites subdomain, you can't change it.

When you create an Experience Cloud site, its path prefix is appended to your Experience Cloud sites domain to create its URL. For example, `https://mycompany.my.site.com/customers`.

For more information, see [Experience Cloud](#).

Salesforce Sites

Salesforce Sites allows you to make any information stored in your org public through a branded URL of your choice. You can also make the site's pages match the look and feel of your company's brand. For example, you can set up sites to publish a catalog of products or to provide a store locator tool. Some features also use Salesforce Sites to deliver functionality. For example, B2B Commerce storefronts are Salesforce Sites.

If enhanced domains are enabled in your org, your My Domain is used as your Salesforce Sites subdomain. The Salesforce Sites URL format is `https://MyDomainName.my.salesforce-sites.com`.

If enhanced domains aren't enabled in your org, the first step in setting up sites is to register a Salesforce Sites domain for your org. Like with My Domain, you pick the subdomain name, and Salesforce adds the domain suffix. The suffix for Salesforce Sites without enhanced domains is `secure.force.com`. For example, if you choose `mycompany-sites` as your sites subdomain, your sites domain is `https://mycompany-sites.secure.force.com`. If you haven't used your My Domain name for your Experience Cloud sites subdomain name, you can use your My Domain name as your Salesforce Sites subdomain name. However, after you choose your Salesforce Sites subdomain, you can't change it.

When you create a site, its name is appended to your sites domain. For example, `https://mycompany-sites.my.salesforce-sites.com/storelocator`.

For more information, see [Salesforce Sites](#).

Custom Domains for Salesforce Sites and Experience Cloud Sites

Custom domains allow you to use a domain that you own, such as `https://www.example.com`, to host externally-facing content from your Experience Cloud sites and Salesforce Sites. Although your Salesforce org provides the content, it's served on your custom domain, providing a clear branded experience for your users.

This feature is especially useful if you own multiple brands and want them to share content. For example, let's say you have a parent company with two distinct brands. Each brand has its own registered domain, and you want them both to point to the parent website. With custom domains, you can point both brand domains to a single parent website with content from your Salesforce org.

For more information on custom domains, see [Custom Domains](#).

SEE ALSO:

[My Domain](#)

[Salesforce Sites](#)

[Experience Cloud](#)

[Custom Domains](#)

What Is My Domain?

Showcase your company's brand with your My Domain name. That My Domain name is used as your org-specific subdomain in Salesforce login and application URLs. For example,

`https://mycompany.my.salesforce.com` and

`https://mycompany.my.site.com`. Learn about the benefits of My Domain, including a custom login page and user login and authentication options.

All orgs get a My Domain by default. If you don't like your org's My Domain name, you can change it.

To get an overview and learn about the benefits of My Domain, watch this video.

 [Watch a video](#)

In addition to `https://login.salesforce.com`, your users can log in to your Salesforce org with your My Domain login URL. This login URL uses a standard format, with your My Domain name as the subdomain. For example, the format for production org login URLs is

`https://MyDomainName.my.salesforce.com`.

With My Domain, you can:

- Highlight your business identity with your unique domain URL.
- Brand your login page, and customize content on the right side of the page.
- Block or redirect page requests that don't use your My Domain name.
- Work in multiple Salesforce orgs in the same browser at the same time.
- Set a custom login policy to determine how users are authenticated.
- Let users log in to Salesforce from the login page with a social account like Google or Facebook.
- Let users log in to your custom external web app with their Salesforce credentials.
- Preserve deep links such as `https://MyDomainName.my.salesforce.com/001/o` during future instance refreshes and org migrations.

With My Domain, Salesforce is enabled as the identity provider, but you can change identity providers. You can also increase security for your org by customizing your domain's login policy.

 **Note:** My Domain URLs for Experience Cloud sites and Salesforce Sites use Salesforce domain suffixes such as `my.site.com` and `salesforce-sites.com`. To use a custom domain such as `https://www.example.com` to serve your org's Experience Cloud sites and Salesforce Sites, see [Custom Domains](#).

SEE ALSO:

[My Domain Provisioning and Deployment](#)

[Configure My Domain Settings](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

My Domain Considerations

When you deploy a change to your My Domain, it's important to understand the impact on URLs across your Salesforce org. Review these considerations about URL changes, feature testing, and reducing the impact to your users.

Plan Your My Domain Change

Whether you change your My Domain to update your brand or to adopt enhanced domains, the URLs that Salesforce hosts for your org change. These changes require planning, coordination, and testing. For high-level steps, recommendations, and checklists, see [Plan for a My Domain Change](#).

Logging In with a My Domain

Your users can log in to your org with its My Domain URL.

Alternatively, users can use these methods to log in to Salesforce.

- <https://login.salesforce.com>, unless an admin prevents logins through the My Domain policies options.
- Your org's instance URL, such as [https://**InstanceName**.salesforce.com/](https://InstanceName.salesforce.com/), unless an admin prevents logins through the My Domain policies options.

My Domain in Non-Production Orgs

My Domain URL formats differ in non-production orgs. All non-production orgs that qualify get partitioned domains, a feature that includes a word related to the org type in the URLs that Salesforce serves for that org. For example, URLs for developer edition orgs include the word `develop` and URLs for sandboxes include the word `sandbox`. Also, `dev-ed` is appended to the My Domain name in Developer Edition orgs. An example login URL for a Developer Edition org is <https://mycompany-dev-ed.develop.my.salesforce.com>.

With partitioned domains, a non-production org other than a Developer edition org and a production org can have the same My Domain name without causing any conflicts. For more information, see [Partitioned Domains](#).

My Domain and Sites Subdomains

With enhanced domains, your My Domain name is used as the subdomain for URLs across your org, including Salesforce Sites and Experience Cloud sites.

If enhanced domains aren't enabled and deployed in your org, your My Domain subdomain isn't used for Experience Cloud sites or Salesforce Sites. You specify separate subdomains when you set up those features.

For more information, see [My Domain URL Formats](#).

 **Note:** To use a custom domain such as <https://www.example.com> to serve your org's Salesforce Sites and Experience Cloud sites, see [Custom Domains](#).

Redirections After a My Domain Change

Each time that you deploy a change to your My Domain details, Salesforce redirects your previous My Domain hostnames to the hostnames for your current My Domain unless you disable those redirects. However, if you change your My Domain more than one time, only the last set of My Domain URLs for your org are redirected. To see if redirects are in place for a previous My Domain, check the Redirections section of the My Domain page. For more information, see [My Domain Redirections](#).

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

Revert a My Domain Deployment

After you save a My Domain change, you can cancel your request before deploying the new domain. On the My Domain Step 3: Deploy New Domain screen, click **Cancel New Domain**.

To revert to your previous My Domain hostnames after you deploy a My Domain change, repeat the steps to change your My Domain. Review and follow the high-level steps, recommendations, and checklists for a My Domain change, see [Plan for a My Domain Change](#).

My Domain and Single Sign-On

For inbound SSO requests, My Domain URLs allow deep linking directly to pages in the org. No changes are required for the identity provider. The Salesforce SAML endpoint `login.salesforce.com` continues to work for SAML and OAUTH requests, even if you deploy My Domain and select **Prevent login from https://login.salesforce.com** in your My Domain Settings.

 **Note:** If you're using external Chatter groups along with SSO for employees, users outside your company are redirected to a SAML identity provider that they can't access. To get SSO to work, migrate external Chatter groups to Experience Cloud sites. Or to allow users to continue to log in through `login.salesforce.com`, don't select the My Domain login policy, **Prevent login from https://login.salesforce.com**.

For more information, see [Set the My Domain Login Policy](#) and [Single Sign-On](#).

For information about updating authentication after your My Domain login URL or sites URL changes, see [Update Authentication After a My Domain Change](#).

Hyperforce and Stabilized My Domain URLs

To avoid instance names and your org's Hyperforce location in your URLs, we recommend that you stabilize your My Domain URLs before moving to Hyperforce. To stabilize your URLs, deploy enhanced domains.

 **Note:** Enhanced domains were enforced in Winter '24. Only a limited number of orgs are using legacy My Domain without enhanced domains.

In a Hyperforce org without enhanced domains enabled, the My Domain setting **Stabilize Visualforce, Experience Builder, Site.com, and content file URLs** controls whether those URLs contain your Salesforce instance and your org's Hyperforce location. If that setting is disabled, the URLs contain your instance name and `sfdc-HyperforceLocation` before the `.force.com` domain suffix. If the setting is enabled, instance names and your org's Hyperforce location aren't included in the URL.

For example, here's the format of a Visualforce URL in a Hyperforce org with enhanced domains:

MyDomainName--PackageName.vf.force.com.

Here's the format of a Visualforce URL with the My Domain setting **Stabilize Visualforce, Experience Builder, Site.com, and content file URLs** disabled:

MyDomainName--PackageName.InstanceName.visual.sfdc-*HyperforceLocation*.force.com.

And here's the format of a Visualforce URL in a Hyperforce org with the My Domain setting **Stabilize Visualforce, Experience Builder, Site.com, and content file URLs** enabled: ***MyDomainName--PackageName***.visualforce.com.

To simplify your org's application URLs, we recommend that you enable and deploy enhanced domains before moving to Hyperforce.

SEE ALSO:

[My Domain](#)

My Domain Provisioning and Deployment

Understand the provisioning and deployment process when you rename your My Domain name, change your My Domain suffix, or enable enhanced domains. Learn about how each step of the process impacts your user's access to Salesforce and why it's important to test these changes in a sandbox.

In each Salesforce org, multiple domains serve content to users. In addition to your My Domain login URL, your org has application URLs on different domains. Here are a few examples.

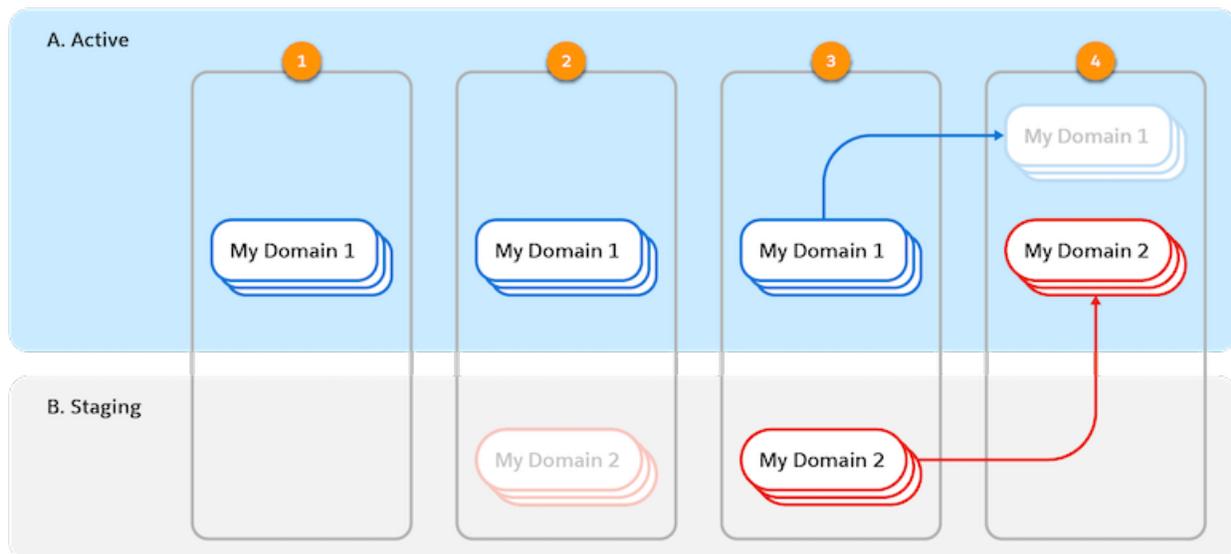
- Lightning pages
- Visualforce pages
- Experience Cloud sites
- Experience Builder for Digital Experiences
- Salesforce Sites
- User-stored content served by Salesforce, such as images and files

When you rename your My Domain or change your My Domain suffix, all those domains are updated. When you enable and deploy enhanced domains, most of the Salesforce application URLs for your org are updated. For more information about all the URLs associated with your org, their formats, and how they change when you enable and deploy enhanced domains, see My Domain URL Formats in Salesforce Help.

My Domain States During a Change

There are three steps to updating your My Domain: save the changes, provision the new domains, and deploy the new domains.

Let's look at an org's state throughout the process. Remember that a My Domain has multiple URLs associated with it, such as the login, Visualforce page, content, and Experience Cloud site URLs.



My Domain changes only become active (A) after they're staged by Salesforce (B) and the admin deploys the change.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

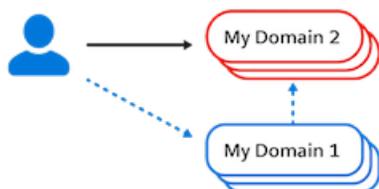
Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

| Step | Accessible Domains | Available Options |
|---|---|---|
| <p>No My Domain changes pending (1).</p> <p>To start the process, you save a change on the My Domain Setup page. For example, you change the My Domain name or enable enhanced domains.</p> <p>User connections are unaffected.</p> | Current My Domain URLs (My Domain 1) | Make a My Domain change and start the provisioning process. |
| <p>Provisioning (2).</p> <p>After you save a change to your My Domain, Salesforce provisions the domains. In other words, we get the new My Domain URLs ready for activation.</p> <p>User connections are unaffected.</p> | Current My Domain URLs (My Domain 1) | <ul style="list-style-type: none"> • Wait for the provisioning process to complete. • To cancel your My Domain change, click Stop Provisioning. |
| <p>Provisioning completed (3).</p> <p>When the provisioning process is complete, the admin who requested the change receives an email. Your new My Domain URLs are ready to be deployed.</p> <p>User connections are unaffected.</p> <p>If anyone visits the new My Domain login URL, they're redirected to the original My Domain login URL. Otherwise, no one can access the new domains at this point.</p> | Current My Domain URLs (My Domain 1) | <ul style="list-style-type: none"> • To deploy your new My Domain URLs, click Deploy New Domain. • To cancel your My Domain changes, click Cancel New Domain. |
| <p>Changes deployed (4).</p> <p>The admin logs in to deploy the updated My Domain. The deployment process also updates the related domains, such as Visualforce pages and Experience Cloud sites.</p> <p>Immediately after the My Domain is deployed, the new My Domain URLs are available to all users.</p> | <ul style="list-style-type: none"> • New My Domain URLs (My Domain 2) • Previous My Domain URLs (My Domain 1) | <ul style="list-style-type: none"> • Disable redirections from your previous My Domain (My Domain 1). • Make a My Domain change and start the provisioning process. |

Until you deploy the changes, all users continue to use the original My Domain (My Domain 1).

When an admin deploys a new My Domain, the admin is logged out of Salesforce. Users are redirected to the new My Domain, which can require logging in again. Everyone can log in again with the new My Domain login URL or, if the My Domain settings allow it, with <https://login.salesforce.com>.

By default, if a user accesses one of the previous My Domain URLs through a link or bookmark, the user is redirected to the corresponding current My Domain URL.



You can disable these redirections through the Routing options on the My Domain Setup page.

Test My Domain Changes

Did you notice something missing from the change process? When did we test the new domains and the related functionality?

Due to the nature of provisioning and deployment, both sets of domains can't be live simultaneously. For this reason, you can't test a My Domain change that's provisioned but not deployed. You can only test My Domain changes after you deploy them.

When you deploy a My Domain change, you have the option of redirecting from the previous URLs to the new URLs. Whether your users access them directly or are redirected to them, everyone accessing the org uses the new URLs. If you don't test your My Domain change before you deploy it, your users can experience an issue in Salesforce due to the change before you learn about it. For example, if your network settings block access to one of your new domains, users can experience connectivity issues or unavailable features.

For this reason, before you update your My Domain in production, we recommend that you always deploy and test My Domain changes in a sandbox. For more information, see [Update Your Org and Test My Domain Changes](#) in Salesforce Help.

SEE ALSO:

[My Domain](#)

[My Domain URL Formats](#)

[My Domain Redirections](#)

[Update Your Org and Test My Domain Changes](#)

Enhanced Domains

Enhanced domains are the current version of My Domain that meets the latest browser requirements. With enhanced domains, all URLs across your org contain your company-specific My Domain name, including URLs for your Experience Cloud sites, Salesforce Sites, Visualforce pages, and content files. This feature changed domain suffixes (the part after the My Domain name) to meet the latest security standards. With no instance names, enhanced My Domain URLs are easier for users to remember and don't change when your org is moved to another Salesforce instance. Because enhanced domains meet the latest browser requirements, this feature was enforced in Winter '24. Watch this video for an overview of enhanced domains, including the possible impact and where to start.

 [Watch a video](#)

For a full list of URL formats and URL format changes when you deploy enhanced domains, see [My Domain URL Format Changes When You Enable Enhanced Domains](#).

[Why Enhanced Domains](#)

When you enable and deploy enhanced domains, most of the application URLs for your Salesforce org change. Those changes require testing and impact public links, such as Experience Cloud sites. Understand why Salesforce requires that all customers adopt this new standard, and learn how enhanced domains meet the latest browser requirements.

[Enhanced Domains Timeline](#)

Salesforce enforced enhanced domains in all orgs in Winter '24. Review the timeline for this feature and when some of the corresponding redirections stop.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Considerations for Enhanced Domains

Before you enable and deploy enhanced domains, understand the prerequisites. Learn about how URLs, including public-facing URLs, change across your org with enhanced domains. Review recommendations for preserving access to your org during the change, learn about redirections, and understand how enhanced domains improve your Experience Cloud sites.

Determine Whether Enhanced Domains Are Enabled

Verify whether enhanced domains are enabled and deployed in your org. Also, when you enable enhanced domains, you can't have a different My Domain change provisioned. If you're not sure whether that applies to you, use the My Domains Setup page to determine your current My Domain state and your options.

Enable Enhanced Domains

To update your Salesforce org's URLs to the latest standards, enable and deploy enhanced domains. With enhanced domains, all URLs across your org contain your company-specific My Domain name, including Experience Cloud sites and Salesforce Sites. Your URLs also remain stabilized when your org is moved to another Salesforce instance.

Troubleshoot Common Errors Related to Enhanced Domains

Enhanced domains apply your org's company-specific My Domain name to all URLs that Salesforce hosts for your org. This feature also changed domain suffixes (the part after the My Domain name) to meet the latest security standards. Learn about the most common issues that you can encounter when testing enhanced domains and how to resolve them.

Why Enhanced Domains

When you enable and deploy enhanced domains, most of the application URLs for your Salesforce org change. Those changes require testing and impact public links, such as Experience Cloud sites. Understand why Salesforce requires that all customers adopt this new standard, and learn how enhanced domains meet the latest browser requirements.

Enhanced domains provide multiple benefits.

- **Branding**—All URLs across your org contain your company-specific My Domain name, including URLs for your Experience Cloud sites, Salesforce Sites, Visualforce pages, and content files.
- **Stability**—With no instance names, your org's URLs remain stabilized when your org is moved to another Salesforce instance.
- **Compliance**—Enhanced domains comply with the latest browser requirements. Specifically, they avoid third-party cookies, otherwise known as cross-site resources.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Third-Party Cookies and Recent Regulations

To understand why Salesforce requires enhanced domains, let's first talk about third-party cookies.

A cookie is a small block of data that a server sends to a user's web browser. The browser can then store the cookie and send it back to the same server during later requests. This data helps web developers give you a more personal and convenient online experience. For example, when you visit a website, cookies allow your account, preferences, and shopping cart to persist from your last visit.

Third-party cookies are stored under a different domain than the domain that you're visiting. These cookies can track you, or your device, across the websites that you visit and display relevant content between websites. For example, you plan for a trip online, and later ads for your vacation destination appear in your social media feed. Third-party cookies also support important functionality, such as a chat hosted by a third-party service provider.

Today, users demand more control over how data collected about them is used, and governments seek to protect the privacy rights of website users. Some laws and regulations that affect cookies include the California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR), and the European Union's pending ePrivacy Regulation (ePR). These laws and regulations require that companies and website operators notify web users about the presence of cookies. These businesses must also let users know what kind of information

is collected and with whom this information is shared. Also, companies and website operators must offer a way to opt out of cookies and data sharing at any time.

Updated Browser Rules for Third-Party Cookies

As a result of regulatory and consumer pressure, the major web browsers block third-party cookies. Today, users can disable a setting in some browsers to allow these cookies, but browser developers state that they intend to permanently block third-party cookies in the future. In particular, Google™ has announced that it plans to phase out these kinds of cookies in Chrome™ in 2024.

Impact on Salesforce Users

Without enhanced domains, Salesforce content could be delivered from multiple domains. When the user's browser blocks third-party cookies, some content in Salesforce could be blocked. For example, a landing page that ends in `lightning.force.com` couldn't load content that was stored in your org and accessed via a URL that ends in `documentforce.com`. The resulting error often mentions "cross-domain cookies" or "cross-site cookies."

The Solution: Enhanced Domains

Enhanced domains make structural changes to the Salesforce domains that serve content. With enhanced domains, all Salesforce content shares a common domain, so the cookies can be shared and the browsers allow access, even when third-party cookies are blocked.

Because enhanced domains allow your users to continue using Salesforce when the browser blocks third-party cookies, they're the future standard and required for all orgs.

When You Can Still See Errors

When you access Salesforce in Classic or visit a Classic page in Lightning, some browsers can flag that interaction as a cross-domain interaction and block the process. Also, users can still experience third-party cookie errors related to embedded Visualforce pages and file-based content under specific conditions.

Here are three specific situations where you can see a message about blocked cross-domain or third-party cookies, even when enhanced domains are deployed.

- When you use a web browser other than Safari 13.1 or later or iOS 14 or later and the browser is configured to block cross-domain cookies, some Salesforce content can fail to load. This issue can occur on Visualforce pages and on Lightning pages with an embedded Visualforce page or embedded file-based content. In this case, the Visualforce page or file-based content can fail to load successfully and the browser displays an error message indicating that the web browser blocked the cookie. To resolve this issue, use Safari 13.1 or later, use iOS 14 or later, or allow cross-domain cookies in your browser.
- When you access a page that contains an embedded Visualforce page, the embedded Visualforce page can display as a blank rectangle. This issue occurs in Salesforce Classic when you use a web browser that blocks cross-domain cookies, such as Safari 13.1 or later or iOS 14 or later. In Lightning Experience, the embedded Visualforce page displays correctly.
- When accessing a Classic page in Lightning, you can receive a warning message about cross-domain cookies. This warning message occurs most often in Setup, because many Setup pages were built in Classic. To resolve this issue, click the link in the warning message to open the Setup page within a new tab or window.

SEE ALSO:

[My Domain](#)

[My Domain URL Formats](#)

[Considerations for Enhanced Domains](#)

[Enable Enhanced Domains](#)

Enhanced Domains Timeline

Salesforce enforced enhanced domains in all orgs in Winter '24. Review the timeline for this feature and when some of the corresponding redirections stop.

To check which release you're running on and when you get the next release, see [Get Your Org Status and Upcoming Maintenance Dates with My Domain](#).

Upcoming Milestone—Winter '25: Redirections for Non-Enhanced Domains Stop

Winter '25 release deployment starts in August 2024 (sandboxes) and September 2024 (production).

When you deploy a new My Domain, including deploying enhanced domains, Salesforce redirects your previous URLs for you. Some non-enhanced domains are retired in Winter '25, thus the redirections for those URLs stop.

Before your org gets this release, enable redirection logging and update all references to your previous non-enhanced domains. After your org gets this release, your previous non-enhanced domains are no longer redirected.

For more information, see [Prepare for the End of Redirections for Non-Enhanced Domains](#).

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

Previous Milestones

- Summer '21—Release deployment started in May 2021 (sandboxes) and June 2021 (production). With this release, enhanced domains were available in Hyperforce orgs and in orgs with a deployed My Domain routed through Salesforce Edge Network. They weren't available in scratch orgs or in Developer Edition orgs.
- Winter '22—Release deployment started in August 2021 (sandboxes) and September 2021 (production). With this release, enhanced domains were available in Hyperforce orgs and in orgs with a deployed My Domain routed through Salesforce Edge Network, including scratch orgs and Developer edition orgs.
- Spring '22—Release deployment started in January 2022 (sandboxes) and February 2022 (production). With this release, enhanced domains were available in all sandbox orgs except Public Cloud sandboxes. For production orgs, enhanced domains were available in Hyperforce orgs and in orgs with a deployed My Domain routed through Salesforce Edge Network.
- Summer '22—In this release, enhanced domains were available in all orgs, including orgs without Hyperforce or Salesforce Edge Network. In June 2022, Public Cloud orgs were the last group of orgs to get the ability to enable enhanced domains. Starting in early July 2022, enhanced domains were enabled by default in new orgs.
- Winter '23—Release deployment started in August 2022 (sandbox) and October 2022 (production). With this release, Salesforce deployed enhanced domains in sandboxes and non-production orgs unless you opted out before the release. Non-production orgs include Developer Edition, demo, free, patch, and scratch orgs, plus Trailblazer Playgrounds. Production orgs were unaffected. Customers retained the ability to disable and enable enhanced domains in this release.
- Spring '23—Release deployment started in January 2023 (sandboxes) and February 2023 (production). With this release, Salesforce deployed enhanced domains in all remaining orgs, including production orgs, unless you opted out of that deployment before the release. Customers retained the ability to disable and enable enhanced domains in this release.
- Summer '23—Release deployment started in May 2023 (sandboxes) and June 2023 (production). With this release, Salesforce deployed enhanced domains in all orgs that didn't have enhanced domains yet. Customers retain the ability to disable and enable enhanced domains in this release.

- Winter '24—Release deployment started in August 2023 (sandboxes) and September 2023 (production). In this release, the Deploy Enhanced Domains release update was enforced. With that enforcement, enhanced domains were deployed in all remaining orgs, and the feature can't be disabled in any org.

SEE ALSO:

[My Domain](#)

[Enhanced Domains](#)

[Plan for a My Domain Change](#)

[My Domain Redirections](#)

Considerations for Enhanced Domains

Before you enable and deploy enhanced domains, understand the prerequisites. Learn about how URLs, including public-facing URLs, change across your org with enhanced domains. Review recommendations for preserving access to your org during the change, learn about redirections, and understand how enhanced domains improve your Experience Cloud sites.

 **Tip:** To get an overview of enhanced domains, watch the  [enhanced domains video](#).

Enforcement

In Winter '24, all orgs got enhanced domains and the feature can't be disabled. For more information, see [Enhanced Domains Timeline](#).

The information in this topic is designed to assist customers who continue to test the changes after deploying enhanced domains.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Plan Your My Domain Change

When you deploy enhanced domains, the URLs that Salesforce hosts for your org change. These changes require planning, coordination, and testing. For high-level steps, recommendations, and checklists, see [Plan for a My Domain Change](#).

Preserve Access to Your Org

When you deploy enhanced domains, login URLs for your sites change. Your My Domain login URL changes when you deploy enhanced domains in a sandbox. Enhanced domains don't change your My Domain login URL in production unless you also change your My Domain name or suffix.

When your My Domain login URL or site URL changes, authentication methods such as SSO and multi-factor authentication (MFA) can stop working. Before you deploy a change to your My Domain, [preserve access](#) for your users and admins.

 **Important:** If you don't follow this guidance before you deploy a change to your My Domain login URL, you can be locked out of your Salesforce org.

URL Changes

When you deploy enhanced domains, all URLs across your org contain your company-specific My Domain name, including Experience Cloud sites and Salesforce sites. Also, your URLs don't change when your org is moved to another Salesforce instance. Here are some example URL formats for a production org with enhanced domains.

| TYPE | ENHANCED DOMAIN URL FORMAT |
|---|---|
| Login | MyDomainName .my.salesforce.com |
| Experience Cloud sites | MyDomainName .my.site.com |
| Salesforce Sites | MyDomainName .my.salesforce-sites.com |
| Visualforce pages | MyDomainName--PackageName .vf.force.com |
| Sandbox Login | MyDomainName--SandboxName .sandbox.my.salesforce.com |
| Experience Cloud sites in a sandbox org | MyDomainName--SandboxName .sandbox.my.site.com |

If your org was created before October 2020, you didn't get a My Domain by default. In that case, your users accessed Salesforce with URLs that contained your instance name but not your My Domain name. If you hard-coded any of those old URLs in your org, update them to the enhanced domain format.

For a full list of enhanced domain URL formats and tables listing the changed formats when you deploy enhanced domains, see [My Domain URL Formats](#).

Because your org's URLs change, we recommend that you test your org's functionality in a sandbox with enhanced domains before enabling this feature in production. Pay particular attention to customizations that reference your old URLs. Note the changes required to complete successful tests, then use that list when deploying your My Domain with enhanced domains in production. For more information and guidance on the areas to update, see [Update Your Org and Test My Domain Changes](#).

Differences Between Sandbox and Production

When you deploy enhanced domains, your production My Domain login URL format, **MyDomainName**.my.salesforce.com, doesn't change unless you also change your My Domain name or suffix. However, many other URLs change.

When you enable enhanced domains in a sandbox, the word "sandbox" is added to all My Domain URLs, including the org's My Domain login URL: **MyDomainName--SandboxName**.sandbox.my.salesforce.com. Similarly, the URL for your Lightning pages also changes in a sandbox, but not in production.

Therefore, some changes are required in your sandbox to test enhanced domains that aren't required in production unless you also change your My Domain name or suffix. The changes that apply only when your My Domain login URL changes are called out on [Update Your Org for My Domain Changes](#) in Salesforce Help. If you deploy enhanced domains in production without changing your My Domain name or suffix, those tasks don't apply.

Changes to Public-Facing URLs

When you deploy enhanced domains, the URLs for your Experience Cloud sites and Salesforce Sites change. With enhanced domains, these URLs include your My Domain name. For this change, there are two important considerations.

- Your My Domain name is now externally exposed. If Experience Cloud sites or Salesforce Sites are enabled, the default Salesforce URL contains your My Domain name. For example, **MyDomainName**.my.site.com for Experience Cloud sites. If your current My Domain name reflects an internal-only brand, you have two options.
 - (Recommended.) Use a custom domain such as `www.externalbrandname.com` to serve the Experience Cloud site or Salesforce Site. For more information, see [Custom Domains](#).
 - Rename your My Domain so that it reflects your external brand when you deploy enhanced domains. Renaming your My Domain changes your login URL and other URLs that Salesforce hosts for your org.

- These URLs can be used outside of Salesforce. Identify all locations where these public-facing URLs are used. For example, a site URL can be used on your website, social media pages, marketing materials, and templates, such as email signatures and automated responses. Then create a plan to update each location and announce the change to your users and customers.

Redirection of Non-Enhanced My Domain URLs

Before you deploy enhanced domains, consider the impact on any existing My Domain hostname redirections.

Salesforce only redirects your last set of previous My Domain URLs. If you previously changed your My Domain, your previous My Domain URLs redirect to your current My Domain URLs unless you disable those redirects. When you deploy another change to your My Domain, including enabling enhanced domains, existing redirections stop, and Salesforce redirects the My Domains in place before the latest deployment instead.

To see if redirects are in place for a previous My Domain, check the Redirections section of the My Domain page. Salesforce stops redirections for some non-enhanced hostnames in Winter '25, starting in August 2024 for sandboxes. For more information on redirections and how to determine which My Domain hostnames are being redirected for your org, see [My Domain Redirections](#).

Experience Cloud Content Delivery Network (CDN)

When you deploy enhanced domains, the format of your Experience Cloud site URL changes from

ExperienceCloudSitesSubdomainName.force.com to ***MyDomainName***.my.site.com. Your *.my.site.com domain includes the Experience Cloud Content Delivery Network (CDN). The Experience Cloud CDN reduces the page load time and provides availability features for your Experience Cloud sites. For more information, see [Content Delivery Networks \(CDNs\) and Salesforce](#).

This change requires some adjustments to your configuration. For details, see [Update Your Org for My Domain Changes](#).

If you disable enhanced domains, your Experience Cloud site URL reverts to its previous

ExperienceCloudSitesSubdomainName.force.com format and it no longer uses the Experience Cloud CDN. Disabling enhanced domains can require reversing the updates outlined on [Update Your Org for My Domain Changes](#).

Testing Packaged-Delivered Functionality

[AppExchange](#) is the Salesforce marketplace, offering thousands of solutions and services that extend Salesforce. Through AppExchange, Salesforce and our partners offer those solutions through packages. Often those packages include functionality that references your org's URLs. For example, for example, a package-delivered Visualforce page can contain links to your sites, content, or other Visualforce pages. In most cases, you can't edit those package-delivered components. If you update one of those components, a future package update can overwrite your changes.

We recommend that package developers use relative paths or dynamically generated hostnames to build any links. If they follow that approach, updated links work after a My Domain change, such as enabling enhanced domains. However, it's possible that a package developer included a hard-coded link in their package. If you find an issue with components or functionality delivered by a package, contact the package developer. Make them aware of the issue so that they can publish a new version of their package that works with enhanced domains and partitioned domains.

Third-Party Cookie Errors

Enhanced domains comply with the latest browser requirements. Specifically, they avoid third-party cookies, otherwise known as cross-site resources. However, in certain scenarios, you can still see errors related to cross-domain and third-party cookies in Salesforce, even when enhanced domains are deployed.

To avoid these errors, we recommend that you use Lightning Experience. Also, let your users know that they can receive a warning that requires them to open the page in another tab or window, especially on Setup pages.

For more information on the conditions that can cause these errors, see [Why Enhanced Domains](#).

Disable Enhanced Domains

Now that enhanced domains have been enforced, you can't disable the feature.

Potential Impact

If enhanced domains aren't deployed in your Salesforce org before Salesforce deploys the feature for you, here are some issues that can arise.

- Users can experience errors when attempting to access Salesforce, including but not limited to Experience Cloud sites, Salesforce Sites, and Visualforce pages.
- Some embedded content stored in Salesforce no longer appears.
- Third-party applications can lose access to your data.
- Single sign-on integrations with sandboxes can fail.
- Single sign-on integrations with orgs using the `*.cloudforce.com` and `*.database.com` domain suffixes can fail.

For more information about the issues you can encounter, see [Troubleshoot Common Errors Related to Enhanced Domains](#) in Salesforce Help.

To avoid these issues, we recommend that you test and deploy enhanced domains in a sandbox and deploy enhanced domains in production before Salesforce deploys the feature for you. For more information about what happens in each release, see [Enhanced Domains Timeline](#).

SEE ALSO:

[My Domain](#)

[Enable Enhanced Domains](#)

Determine Whether Enhanced Domains Are Enabled

Verify whether enhanced domains are enabled and deployed in your org. Also, when you enable enhanced domains, you can't have a different My Domain change provisioned. If you're not sure whether that applies to you, use the My Domains Setup page to determine your current My Domain state and your options.

In Winter '24, all orgs got enhanced domains and the feature can't be disabled. For more information, see [Enhanced Domains Timeline](#).

Determine Your Current My Domain State

The My Domain Setup page shows your current My Domain URL and indicates whether enhanced domains are enabled or deployed in your org. If a My Domain change is in progress, you can cancel the pending change.

To view the My Domain Setup page, from Setup, in the Quick Find box, enter *My Domain*, and then select **My Domain**.

- If you see Step 2: Provisioning in Progress, a My Domain is being provisioned. Typically, the provisioning process completes in 24 hours or less.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

My Domain Settings [Help for this Page](#)

A My Domain showcases your company's brand and keeps your data more secure by making your Salesforce org's URL customer-specific. A My Domain is also required for many Salesforce features.

Set up a My Domain in three steps:

1. Choose and register a My Domain
- 2. Salesforce provisions your new domain**
3. Deploy your new domain to users

Step 2: Provisioning in Progress

Your new domain is being provisioned. After provisioning completes, deploy your new domain for your changes to take effect. You will receive an email when the provisioning is complete.

| | |
|----------------|--|
| Current domain | mycompany.my.salesforce.com with enhanced domains |
| New domain | mynewbrand.my.salesforce.com with enhanced domains |

[Stop Provisioning](#)

To enable enhanced domains, you can't have a different My Domain change in progress. If you don't want the change shown on the screen or it has been more than 24 hours, click **Stop Provisioning** to reset the process.

- If you see Step 3: Deploy Your New Domain, a My Domain has been provisioned, but the My Domain isn't yet deployed.

My Domain Settings [Help for this Page](#)

A My Domain showcases your company's brand and keeps your data more secure by making your Salesforce org's URL customer-specific. A My Domain is also required for many Salesforce features.

Set up a My Domain in three steps:

1. Choose and register a My Domain
2. Salesforce provisions your new domain
- 3. Deploy your new domain to users**

Step 3: Deploy Your New Domain

Your new domain has been provisioned and is ready to be deployed to users.

| | |
|----------------|--|
| Current domain | mycompany.my.salesforce.com with enhanced domains |
| New domain | mynewbrand.my.salesforce.com with enhanced domains |

[Keep Current Domain](#) [Deploy New Domain](#)

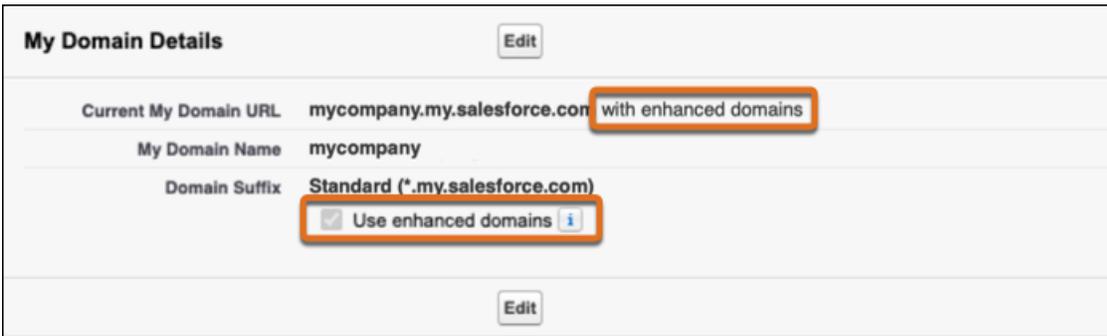
The current domain and new domain fields indicate whether enhanced domains are enabled on each My Domain.

- To reset the process, click **Cancel New Domain**.
- If you're satisfied with your new domain and that domain uses enhanced domains, you can click **Deploy New Domain** to make it available to your users.

 **Warning:** Deploying a new My Domain can disrupt user access. Before updating production, we recommend that you test all My Domain changes in a sandbox. For more information, see [Update Your Org and Test My Domain Changes](#).

- If you see My Domain Details, you don't have any pending My Domain changes. Your current My Domain login URL is shown in the My Domain Details section. The current My Domain URL field also indicates whether enhanced domains are enabled.

Here's an example of the My Domain Details section in an org with enhanced domains deployed.

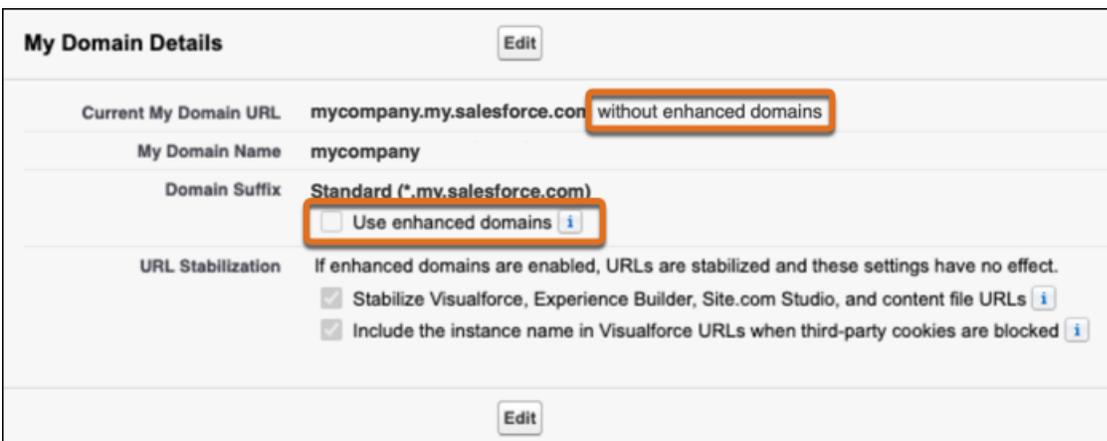


The screenshot shows the 'My Domain Details' section. The 'Current My Domain URL' is 'mycompany.my.salesforce.com with enhanced domains'. The 'My Domain Name' is 'mycompany'. The 'Domain Suffix' is 'Standard (*.my.salesforce.com)'. The 'Use enhanced domains' checkbox is checked. There are 'Edit' buttons at the top and bottom of the section.

The Current My Domain URL field includes the phrase “with enhanced domains,” and the **Use enhanced domains option** is enabled.

 **Note:** If the Current My Domain URL includes the phrase “without enhanced domains,” enhanced domains aren't deployed, even if the **Use enhanced domains** option is enabled.

And here's an example of the My Domain Details section in an org without enhanced domains.



The screenshot shows the 'My Domain Details' section. The 'Current My Domain URL' is 'mycompany.my.salesforce.com without enhanced domains'. The 'My Domain Name' is 'mycompany'. The 'Domain Suffix' is 'Standard (*.my.salesforce.com)'. The 'Use enhanced domains' checkbox is unchecked. There are 'Edit' buttons at the top and bottom of the section. Below the domain settings, there is a 'URL Stabilization' section with two checked options: 'Stabilize Visualforce, Experience Builder, Site.com Studio, and content file URLs' and 'Include the instance name in Visualforce URLs when third-party cookies are blocked'.

The Current My Domain URL includes the phrase “without enhanced domains,” and the **Use enhanced domains** option isn't enabled.

SEE ALSO:

[Enable Enhanced Domains](#)

Enable Enhanced Domains

To update your Salesforce org's URLs to the latest standards, enable and deploy enhanced domains. With enhanced domains, all URLs across your org contain your company-specific My Domain name, including Experience Cloud sites and Salesforce Sites. Your URLs also remain stabilized when your org is moved to another Salesforce instance.

These steps apply only if your org doesn't use enhanced domains. To determine if enhanced domains are enabled in your org, see [Determine Whether Enhanced Domains Are Enabled](#).

Before you enable and deploy enhanced domains, review the [considerations](#) for this feature.

 **Note:** Enhanced domains change URLs formats across your org. We recommend that you test this feature in a sandbox before you deploy it in production. To review the high-level steps, the recommended practices, and how to reduce the impact on your users and customers, see [Plan for a My Domain Change](#) in Salesforce Help.

1. From Setup, in the Quick Find box, enter *My Domain*, and then select **My Domain**.
2. Under My Domain Details, select **Edit**.

EDITIONS

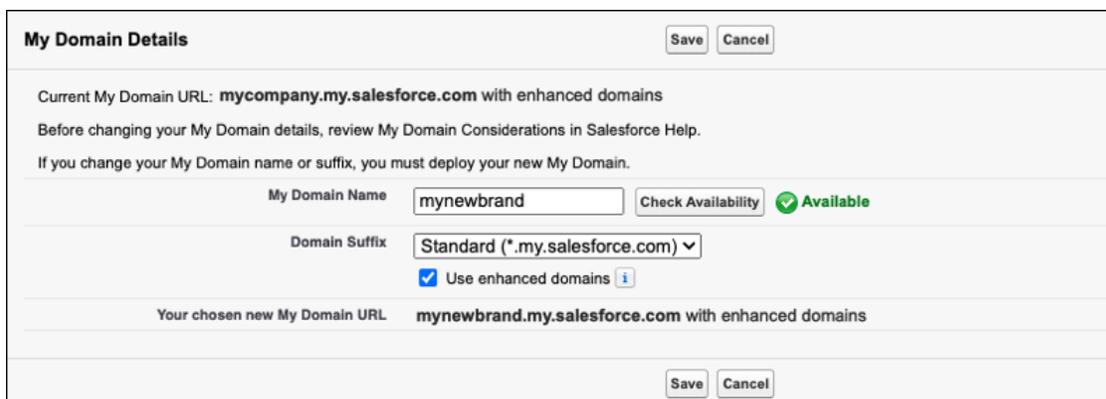
Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To edit My Domain settings:

- Customize Application



My Domain Details Save Cancel

Current My Domain URL: **mycompany.my.salesforce.com** with enhanced domains

Before changing your My Domain details, review My Domain Considerations in Salesforce Help.

If you change your My Domain name or suffix, you must deploy your new My Domain.

My Domain Name: Check Availability Available

Domain Suffix: ▼

Use enhanced domains i

Your chosen new My Domain URL: **mynewbrand.my.salesforce.com** with enhanced domains

Save Cancel

3. If more suffixes are available for your org's My Domain, a suffix dropdown list appears. Enhanced domains can only be enabled for the Standard suffix.
4. Select **Use enhanced domains**.
5. Save your changes.

 **Note:** To use enhanced domains and comply with the Deploy Enhanced Domains release update, deploy your updated My Domain.

Next Steps:

1. Salesforce provisions the URLs for your My Domain with enhanced domains. The provisioning process usually finishes in a few minutes, but it can take up to 24 hours. You receive an email when your My Domain with enhanced domains is ready to be deployed and tested.
2. Review the [My Domain URL Format Changes When You Enable Enhanced Domains](#).
3. [Deploy your new My Domain, update your org, and test the changes](#).

4. Update external-facing links, such as publicly available Experience Cloud sites and Salesforce Sites. For example, a site URL can be used on your website, social media pages, marketing materials, and templates, such as email signatures and automated responses. Create a plan to update each location and announce the change to your users and customers.
5. After you complete testing, help your users get started using your new enhanced domain URLs by providing links to pages that they use frequently, such as your Experience Cloud sites. Encourage them to update their bookmarks the first time they're redirected and to use any updated templates.
6. After you complete your testing and enable this feature in production, review the Deploy Enhanced Domains release update and complete it if appropriate.

SEE ALSO:

[My Domain](#)

[Salesforce Edge Network](#)

Troubleshoot Common Errors Related to Enhanced Domains

Enhanced domains apply your org's company-specific My Domain name to all URLs that Salesforce hosts for your org. This feature also changed domain suffixes (the part after the My Domain name) to meet the latest security standards. Learn about the most common issues that you can encounter when testing enhanced domains and how to resolve them.

Here are common issues that you can encounter after you deploy enhanced domains. For more information on the related updates, see [Update Your Org for My Domain Changes](#).

 **Note:** This list of potential issues isn't comprehensive. We recommend that you verify your configuration by testing enhanced domains in a sandbox before you deploy enhanced domains in production.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Potential Issues in Any Org

| Behavior | Related Updates |
|--|--|
| Errors when attempting to access Salesforce pages, including but not limited to: Experience Cloud sites, Salesforce Sites, Visualforce pages, and content. | <ul style="list-style-type: none"> • Update your allowlists, trusted domains, permitted domains, and other hostname-based restrictions. • Update hard-coded references to your old URLs. • Update your version of the Mobile Publisher for Experience Cloud app. |
| Users can't access Experience Cloud sites or Salesforce Sites. | <ul style="list-style-type: none"> • Update IP-based restrictions to include the IPv6 range. • Update authentication (SSO, MFA, named credentials). • Update the identity providers on your login page. • Update hard-coded references to your site URL. • Update trusted domains for inline frames. • Update network-level restrictions that specify only IP addresses. |
| The custom domain that serves your Experience Cloud site or Salesforce Sites stops working. | Update the domain configuration as required. |

| Behavior | Related Updates |
|---|--|
| Open CTI (Computer-Telephony Integration) or Click to Dial stops working. | <ul style="list-style-type: none"> • Add your new Visualforce URL to your telephony provider's allowlists. • Update any hard-coded references to your Visualforce URLs in your configuration. Whenever possible, update these to relative URLs instead. <p>For more information, see the Knowledge Article, Enhanced Domains and Open CTI with Visualforce (Spring '23).</p> |
| External integrations, external software, or connected apps can't access your Experience Cloud sites or Salesforce Sites. | <ul style="list-style-type: none"> • Update authentication to use your new site login URL. • Work with the third party to update their configuration to use your new site login URL. • Work with the third parties to ensure that they support Server Name Indication (SNI). |
| Users can't access enablement sites (myTrailhead) that use your sites URL that ends in *.force.com. | Contact Salesforce Customer Support to update your authentication provider with your new sites login URL. |
| Images stored in Salesforce fail to load on internal sites, emails, or external sites. | <ul style="list-style-type: none"> • Update the URL references to content stored in Salesforce. • Update badge and image URLs in enablement sites (myTrailhead). |
| Some functionality within installed packages from AppExchange stops working. | Verify whether the package has been updated and install a patch or version that supports enhanced domains. |

Potential Issues When Your My Domain Login URL Changes

When your My Domain login URL changes, you can encounter these additional common issues. Your My Domain login URL changes when you deploy enhanced domains in a sandbox and when you change your My Domain name. Also, if you currently use the *.cloudforce.com or *.database.com suffix, you adopt the standard *.my.salesforce.com suffix as part of deploying enhanced domains, and these issues can arise.

| Behavior | Related Updates |
|--|--|
| Users and processes can't access your Salesforce org. | <ul style="list-style-type: none"> • Update authentication (SSO, MFA, named credentials). • Update the identity providers on your login page. • Update hard-coded references to your My Domain login URL. |
| Third-party connected apps and integrations fail to connect to your org or site. | <ul style="list-style-type: none"> • Update authentication. • Update hard-coded references to your My Domain login URL. • Ensure that third parties can process the redirect header from Salesforce. |
| A Messaging for Web deployment that was previously published no longer appears to your customer. | Republish all pre-existing deployments of Messaging for In-App. |

| Behavior | Related Updates |
|--|---|
| Users can't access enablement sites (myTrailhead) that use your My Domain login URL. | Contact Salesforce Customer Support to update your authentication provider with your new My Domain login URL. |
| Service Cloud Voice stops working. | <ul style="list-style-type: none"> Work with your telephony provider to update your configuration with your new URLs. Update the allowlist in Amazon Connect with your new Visualforce URL. |

SEE ALSO:

[Enhanced Domains](#)

[Update Authentication After a My Domain Change](#)

Partitioned Domains

With partitioned domains, My Domain hostnames for your Developer Edition org, demo org, patch org, sandbox, scratch org, or Trailhead Playground include a word related to the org type. For example, partitioned domains for Developer Edition and patch orgs include the word develop. Partitioned domains allow Salesforce to maximize the availability of your orgs by gradually rolling out delivery changes. And it's easier to identify an org by a URL when the domain is partitioned.

Partitioned Domains are available in Developer Edition orgs, demo orgs, patch orgs, scratch orgs, and Trailhead Playgrounds with enhanced domains. Sandboxes with enhanced domains are always partitioned.

Only the sandbox partition is available in orgs on the GIA Hyperforce instance and in Public Cloud orgs. Otherwise, if you use Salesforce Edge Network, only the sandbox, patch, demo, and develop partitions are available.

The scratch partition can be available in orgs on Salesforce Edge Network before Summer '24. For updates about the availability of this feature, join the [My Domain and Enhanced Domains](#) group in the Trailblazer Community.

 **Note:** Qualifying new orgs get partitioned domains by default, and you can't disable this feature in those orgs.

Partitioned domains allow Salesforce to gradually roll out service delivery changes by org type. For example, Developer Edition orgs can get an update separately from production orgs. This staggered approach maximizes the availability of production and sandbox orgs.

My Domain uses partitioned domains for new orgs of these types, and you can enable partitioned domains in these types.

EDITIONS

Available in: both Salesforce Classic (**not available in all orgs**) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

| Org Type | Partition Name |
|-------------------------|----------------|
| Developer Edition orgs | develop |
| Demo orgs | demo |
| Patch orgs | patch |
| Sandboxes | sandbox |
| Scratch orgs | scratch |
| Trailblazer Playgrounds | trailblaze |

For example, the My Domain login URL format for a partitioned Developer Edition org is `https://MyDomainName.develop.my.salesforce.com`.

[Enable Partitioned Domains](#)

To maximize the availability of your orgs, enable and deploy partitioned domains for your My Domain in your existing Developer Edition org, demo org, patch org, sandbox, scratch org, or Trailhead Playground. Partitioned domains allow Salesforce to gradually roll out service delivery changes by org type. When a domain is partitioned, it includes a word related to the org type, which also makes it easier to identify an org by a URL.

[Partitioned Domains for Demo Orgs](#)

Review the login and application domains that Salesforce hosts for demo orgs with partitioned domains.

[Partitioned Domains for Developer Edition Orgs](#)

Review the login and application domains that Salesforce hosts for Developer Edition orgs with partitioned domains. New Developer Edition and patch orgs are partitioned by default.

[Partitioned Domains for Patch Orgs](#)

Review the login and application domains that Salesforce hosts for patch orgs with partitioned domains.

[Partitioned Domains for Sandboxes](#)

Sandboxes with enhanced domains use the sandbox partition. Review the login and application domains that Salesforce hosts for sandboxes.

[Partitioned Domains for Scratch Orgs](#)

Review the login and application domains that Salesforce hosts for scratch orgs with partitioned domains. New scratch orgs are partitioned by default.

[Partitioned Domains for Trailhead Playgrounds](#)

Review the login and application domains that Salesforce hosts for Trailhead Playgrounds with partitioned domains. New Trailhead Playgrounds are partitioned by default.

SEE ALSO:

[My Domain](#)

[Enhanced Domains](#)

Enable Partitioned Domains

To maximize the availability of your orgs, enable and deploy partitioned domains for your My Domain in your existing Developer Edition org, demo org, patch org, sandbox, scratch org, or Trailhead Playground. Partitioned domains allow Salesforce to gradually roll out service delivery changes by org type. When a domain is partitioned, it includes a word related to the org type, which also makes it easier to identify an org by a URL.

Partitioned Domains are available in Developer Edition orgs, demo orgs, patch orgs, scratch orgs, and Trailhead Playgrounds with enhanced domains. Sandboxes with enhanced domains are always partitioned.

Only the sandbox partition is available in orgs on the GIA Hyperforce instance and in Public Cloud orgs. Otherwise, if you use Salesforce Edge Network, only the sandbox, patch, demo, and develop partitions are available.

The scratch partition can be available in orgs on Salesforce Edge Network before Summer '24. For updates about the availability of this feature, join the [My Domain and Enhanced Domains](#) group in the Trailblazer Community.

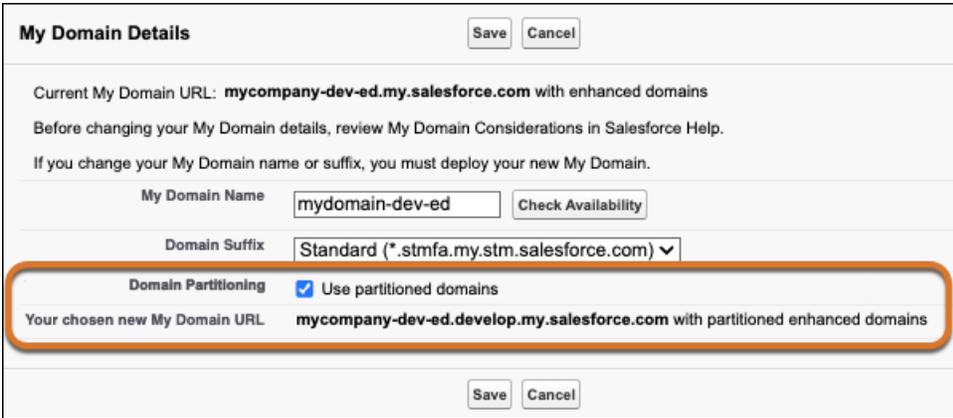
Qualifying new orgs get partitioned domains by default, and you can't disable this feature in those orgs.

 **Warning:** Before you deploy partitioned domains, update your allowlists to ensure that your users can connect to the partitioned domains.

Partitioned domains change URL formats across your org. To review the high-level steps and the recommended practices for a My Domain change, plus how to reduce the impact on your users and customers, see [Plan for a My Domain Change](#).

1. From Setup, in the Quick Find box, enter *My Domain*, and then select **My Domain**.
2. In the My Domain Details section, click **Edit**.
3. Select **Use partitioned domains**.

You can preview your new My Domain login URL at the bottom of the screen.



My Domain Details Save Cancel

Current My Domain URL: **mycompany-dev-ed.my.salesforce.com** with enhanced domains

Before changing your My Domain details, review My Domain Considerations in Salesforce Help.

If you change your My Domain name or suffix, you must deploy your new My Domain.

My Domain Name Check Availability

Domain Suffix ▼

Domain Partitioning Use partitioned domains

Your chosen new My Domain URL **mycompany-dev-ed.develop.my.salesforce.com** with partitioned enhanced domains

Save Cancel

This option isn't available in sandboxes. Sandboxes with enhanced domains are always partitioned and use the "sandbox" partition. Otherwise, if you don't see the Use partitioned domains option, your org doesn't qualify for this feature.

4. Save your changes.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To edit My Domain settings:

- Customize Application

When you save your changes, Salesforce provisions the URLs for your My Domain with partitioned enhanced domains. The provisioning process usually finishes in a few minutes, but it can take up to 24 hours. You receive an email when your My Domain with partitioned enhanced domains is ready to be deployed and tested.

When you receive the email that your domain is ready to be deployed, [deploy your new My Domain, update your org, and test the changes](#). After you complete testing, help your users of the non-production org get started. Provide links to pages that they use frequently and encourage them to update their bookmarks the first time that they're redirected.

SEE ALSO:

- [My Domain](#)
- [Partitioned Domains](#)
- [Enhanced Domains](#)

Partitioned Domains for Demo Orgs

Review the login and application domains that Salesforce hosts for demo orgs with partitioned domains.

 **Note:** Partitioned Domains require enhanced domains. The demo partition isn't available in orgs on the GIA Hyperforce instance or in Public Cloud orgs. Qualifying new orgs get partitioned domains by default, and you can't disable this feature in those orgs.

Here are the domains that Salesforce hosts for demo orgs with partitioned domains. To better understand the purpose of each hostname type and whether it applies to you, see [My Domain Hostnames](#) in Salesforce Help.

| URL TYPE | URL FORMAT |
|---|--|
| Login | <i>MyDomainName</i> .demo.my.salesforce.com |
| Application Page or Tab | <i>MyDomainName</i> .demo.my.salesforce.com/ <i>PageID</i> |
| Content (files) | <i>MyDomainName</i> .demo.file.force.com |
| Content Management System (CMS) public channels | <i>MyDomainName</i> .demo.cdn.salesforce-experience.com |
| Email tracking (reserved for future use) | <i>MyDomainName</i> .demo.my.sfdcopens.com |
| Experience Cloud Sites | <i>MyDomainName</i> .demo.my.site.com |
| Experience Builder | <i>MyDomainName</i> .demo.builder.salesforce-experience.com |
| Experience Builder Preview | <i>MyDomainName</i> .demo.preview.salesforce-experience.com |

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Developer** edition

| URL TYPE | URL FORMAT |
|---|---|
| Experience Builder Live Preview | MyDomainName .demo.live-preview.salesforce-experience.com |
| Lightning | MyDomainName .demo.lightning.force.com |
| Lightning Container Component | MyDomainName--PackageName .demo.container.force.com ¹ |
| Salesforce Sites | MyDomainName .demo.my.salesforce-sites.com |
| Setup Pages | MyDomainName .demo.my.salesforce-setup.com |
| Next generation Omni-Channel engagement (examples: voice and messaging) | MyDomainName .demo.my.salesforce-scrt.com |
| User Content | MyDomainName--UniqueID .demo.my.force-user-content.com |
| User Content on a Government Cloud org | MyDomainName--UniqueID .demo.gia.force-user-content.com |
| User Image (reserved for future use) | MyDomainName--UniqueID .demo.file.force-user-content.com |
| Visualforce | MyDomainName--PackageName .demo.vf.force.com ¹ |

¹ If your installed package is unmanaged, the package name is c

SEE ALSO:

- [My Domain](#)
- [Partitioned Domains](#)

Partitioned Domains for Developer Edition Orgs

Review the login and application domains that Salesforce hosts for Developer Edition orgs with partitioned domains. New Developer Edition and patch orgs are partitioned by default.

 **Note:** Partitioned Domains require enhanced domains. The developer partition isn't available in orgs on the GIA Hyperforce instance or in Public Cloud orgs. Qualifying new orgs get partitioned domains by default, and you can't disable this feature in those orgs.

If partitioned domains were enabled in a patch org before Winter '24, that org uses the develop partition.

Here are the domains that Salesforce hosts for Developer Edition orgs with partitioned domains. To better understand the purpose of each hostname type and whether it applies to you, see [My Domain Hostnames](#) in Salesforce Help.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Developer edition**

| URL TYPE | URL FORMAT |
|---|--|
| Login | MyDomainName .develop.my.salesforce.com |
| Application Page or Tab | MyDomainName .develop.my.salesforce.com/ PageID |
| Content (files) | MyDomainName .develop.file.force.com |
| Content Management System (CMS) public channels | MyDomainName .develop.cdn.salesforce-experience.com |
| Email tracking (reserved for future use) | MyDomainName .develop.my.sfdcopens.com |
| Experience Cloud Sites | MyDomainName .develop.my.site.com |
| Experience Builder | MyDomainName .develop.builder.salesforce-experience.com |
| Experience Builder Preview | MyDomainName .develop.preview.salesforce-experience.com |
| Experience Builder Live Preview | MyDomainName .develop.live-preview.salesforce-experience.com |
| Lightning | MyDomainName .develop.lightning.force.com |
| Lightning Container Component | MyDomainName--PackageName .develop.container.force.com ¹ |
| Salesforce Sites | MyDomainName .develop.my.salesforce-sites.com |
| Setup Pages | MyDomainName .develop.my.salesforce-setup.com |
| Next generation Omni-Channel engagement (examples: voice and messaging) | MyDomainName .develop.my.salesforce-scrt.com |
| User Content | MyDomainName--UniqueID .develop.my.force-user-content.com |
| User Content on a Government Cloud org | MyDomainName--UniqueID .develop.gia.force-user-content.com |
| User Image (reserved for future use) | MyDomainName--UniqueID .develop.file.force-user-content.com |
| Visualforce | MyDomainName--PackageName .develop.vf.force.com ¹ |

¹ If your installed package is unmanaged, the package name is `c`

SEE ALSO:

[My Domain](#)
[Partitioned Domains](#)
[Enhanced Domains](#)
[My Domain](#)
[Partitioned Domains](#)

Partitioned Domains for Patch Orgs

Review the login and application domains that Salesforce hosts for patch orgs with partitioned domains.

 **Note:** Partitioned Domains require enhanced domains. The patch partition isn't available in orgs on the GIA Hyperforce instance or in Public Cloud orgs. Qualifying new orgs get partitioned domains by default, and you can't disable this feature in those orgs.

If partitioned domains were enabled in a patch org before Winter '24, that org uses the develop partition.

Here are the domains that Salesforce hosts for patch orgs with partitioned domains. To better understand the purpose of each hostname type and whether it applies to you, see [My Domain Hostnames](#) in Salesforce Help.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Developer** edition

| URL TYPE | URL FORMAT |
|---|---|
| Login | <i>MyDomainName</i> .patch.my.salesforce.com |
| Application Page or Tab | <i>MyDomainName</i> .patch.my.salesforce.com/ <i>PageID</i> |
| Content (files) | <i>MyDomainName</i> .patch.file.force.com |
| Content Management System (CMS) public channels | <i>MyDomainName</i> .patch.cdn.salesforce-experience.com |
| Email tracking (reserved for future use) | <i>MyDomainName</i> .patch.my.sfdcopens.com |
| Experience Cloud Sites | <i>MyDomainName</i> .patch.my.site.com |
| Experience Builder | <i>MyDomainName</i> .patch.builder.salesforce-experience.com |
| Experience Builder Preview | <i>MyDomainName</i> .patch.preview.salesforce-experience.com |
| Experience Builder Live Preview | <i>MyDomainName</i> .patch.live-preview.salesforce-experience.com |
| Lightning | <i>MyDomainName</i> .patch.lightning.force.com |

| URL TYPE | URL FORMAT |
|---|--|
| Lightning Container Component | MyDomainName--PackageName .patch.container.force.com ¹ |
| Salesforce Sites | MyDomainName .patch.my.salesforce-sites.com |
| Setup Pages | MyDomainName .patch.my.salesforce-setup.com |
| Next generation Omni-Channel engagement (examples: voice and messaging) | MyDomainName .patch.my.salesforce-scr.com |
| User Content | MyDomainName--UniqueID .patch.my.force-user-content.com |
| User Content on a Government Cloud org | MyDomainName--UniqueID .patch.gia.force-user-content.com |
| User Image (reserved for future use) | MyDomainName--UniqueID .patch.file.force-user-content.com |
| Visualforce | MyDomainName--PackageName .patch.vf.force.com ¹ |

¹ If your installed package is unmanaged, the package name is c

SEE ALSO:

[My Domain](#)

[Partitioned Domains](#)

Partitioned Domains for Sandboxes

Sandboxes with enhanced domains use the sandbox partition. Review the login and application domains that Salesforce hosts for sandboxes.

 **Note:** Sandboxes with enhanced domains are always partitioned, even though the Use partitioned domains option isn't on the My Domain Setup page in those orgs.

Here are the partitioned domains that Salesforce hosts for sandboxes with enhanced domains. To better understand the purpose of each hostname type and whether it applies to you, see [My Domain Hostnames](#).

My Domain URL Formats for Sandbox Orgs

| URL TYPE | URL FORMAT |
|-------------------------|---|
| Login | MyDomainName--SandboxName .sandbox.my.salesforce.com |
| Application Page or Tab | MyDomainName--SandboxName .sandbox.my.salesforce.com / PageID |
| Content (files) | MyDomainName--SandboxName .sandbox.file.force.com |

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

| URL TYPE | URL FORMAT |
|---|---|
| Content Management System (CMS) public channels | MyDomainName--SandboxName .sandbox.cdn.salesforce-experience.com |
| Email tracking (reserved for future use) | MyDomainName--SandboxName .sandbox.my.sfdcopens.com |
| Experience Cloud Sites | MyDomainName--SandboxName .sandbox.my.site.com |
| Experience Builder | MyDomainName--SandboxName .sandbox.builder.salesforce-experience.com |
| Experience Builder Preview | MyDomainName--SandboxName .sandbox.preview.salesforce-experience.com |
| Experience Builder Live Preview | MyDomainName--SandboxName .sandbox.live-preview.salesforce-experience.com |
| Lightning | MyDomainName--SandboxName .sandbox.lightning.force.com |
| Lightning Container Component | MyDomainName--SandboxName--PackageName .sandbox.container.force.com ¹ |
| Salesforce Sites | MyDomainName--SandboxName .sandbox.my.salesforce-sites.com |
| Setup Pages | MyDomainName--SandboxName .sandbox.my.salesforce-setup.com |
| Next generation Omni-Channel engagement (examples: voice and messaging) | MyDomainName--SandboxName .sandbox.my.salesforce-scrt.com |
| User Content | MyDomainName--SandboxName--UniqueID .sandbox.my.force-user-content.com |
| User Content on a Government Cloud org | MyDomainName--SandboxName--UniqueID .sandbox.gia.force-user-content.com |
| User Image (reserved for future use) | MyDomainName--SandboxName--UniqueID .sandbox.file.force-user-content.com |
| Visualforce | MyDomainName--SandboxName--PackageName .sandbox.vf.force.com ¹ |

¹ If your installed package is unmanaged, the package name is c.

SEE ALSO:

[My Domain](#)

[Partitioned Domains](#)

Partitioned Domains for Scratch Orgs

Review the login and application domains that Salesforce hosts for scratch orgs with partitioned domains. New scratch orgs are partitioned by default.

 **Note:** Partitioned Domains require enhanced domains. The scratch partition isn't available in orgs on the GIA Hyperforce instance, in Public Cloud orgs, or in orgs that use Salesforce Edge Network. Qualifying new orgs get partitioned domains by default, and you can't disable this feature in those orgs.

The scratch partition can be available in orgs on Salesforce Edge Network before Summer '24. For updates about the availability of this feature, join the [My Domain and Enhanced Domains](#) group in the Trailblazer Community.

Here are the domains that Salesforce hosts for scratch orgs with partitioned domains. To better understand the purpose of each hostname type and whether it applies to you, see [My Domain Hostnames](#).

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

| URL TYPE | URL FORMAT |
|---|--|
| Login | MyDomainName .scratch.my.salesforce.com |
| Application Page or Tab | MyDomainName .scratch.my.salesforce.com/ PageID |
| Content (files) | MyDomainName .scratch.file.force.com |
| Content Management System (CMS) public channels | MyDomainName .scratch.cdn.salesforce-experience.com |
| Email tracking (reserved for future use) | MyDomainName .scratch.my.sfdcopens.com |
| Experience Cloud Sites | MyDomainName .scratch.my.site.com |
| Experience Builder | MyDomainName .scratch.builder.salesforce-experience.com |
| Experience Builder Preview | MyDomainName .scratch.preview.salesforce-experience.com |
| Experience Builder Live Preview | MyDomainName .scratch.live-preview.salesforce-experience.com |
| Lightning | MyDomainName .scratch.lightning.force.com |
| Lightning Container Component | MyDomainName--PackageName .scratch.container.force.com ¹ |
| Salesforce Sites | MyDomainName .scratch.my.salesforce-sites.com |
| Setup Pages | MyDomainName .scratch.my.salesforce-setup.com |
| Next generation Omni-Channel engagement (examples: voice and messaging) | MyDomainName .scratch.my.salesforce-scrt.com |

| URL TYPE | URL FORMAT |
|--|---|
| User Content | MyDomainName--UniqueID .scratch.my.force-user-content.com |
| User Content on a Government Cloud org | MyDomainName--UniqueID .scratch.gia.force-user-content.com |
| User Image (reserved for future use) | MyDomainName--UniqueID .scratch.file.force-user-content.com |
| Visualforce | MyDomainName--PackageName .scratch.vf.force.com ¹ |

¹ If your installed package is unmanaged, the package name is c

SEE ALSO:

[My Domain](#)

[Partitioned Domains](#)

Partitioned Domains for Trailhead Playgrounds

Review the login and application domains that Salesforce hosts for Trailhead Playgrounds with partitioned domains. New Trailhead Playgrounds are partitioned by default.

 **Note:** Partitioned Domains require enhanced domains. The trailblaze partition isn't available in orgs on the GIA Hyperforce instance, in Public Cloud orgs, or in orgs that use Salesforce Edge Network. Qualifying new orgs get partitioned domains by default, and you can't disable this feature in those orgs.

Here are the domains that Salesforce hosts for Trailhead Playgrounds with partitioned domains. To better understand the purpose of each hostname type and whether it applies to you, see [My Domain Hostnames](#).

| URL TYPE | URL FORMAT |
|---|--|
| Login | MyDomainName .trailblaze.my.salesforce.com |
| Application Page or Tab | MyDomainName .trailblaze.my.salesforce.com/ PageID |
| Content (files) | MyDomainName .trailblaze.file.force.com |
| Content Management System (CMS) public channels | MyDomainName .trailblaze.cdn.salesforce-experience.com |
| Email tracking (reserved for future use) | MyDomainName .trailblaze.my.sfdcopens.com |
| Experience Cloud Sites | MyDomainName .trailblaze.my.site.com |

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

| URL TYPE | URL FORMAT |
|---|---|
| Experience Builder | MyDomainName .trailblaze.builder.salesforce-experience.com |
| Experience Builder Preview | MyDomainName .trailblaze.preview.salesforce-experience.com |
| Experience Builder Live Preview | MyDomainName .trailblaze.live-preview.salesforce-experience.com |
| Lightning | MyDomainName .trailblaze.lightning.force.com |
| Lightning Container Component | MyDomainName--PackageName .trailblaze.container.force.com ¹ |
| Salesforce Sites | MyDomainName .trailblaze.my.salesforce-sites.com |
| Setup Pages | MyDomainName .trailblaze.my.salesforce-setup.com |
| Next generation Omni-Channel engagement (examples: voice and messaging) | MyDomainName .trailblaze.my.salesforce-scrt.com |
| User Content | MyDomainName--UniqueID .trailblaze.my.force-user-content.com |
| User Content on a Government Cloud org | MyDomainName--UniqueID .trailblaze.gia.force-user-content.com |
| User Image (reserved for future use) | MyDomainName--UniqueID .trailblaze.file.force-user-content.com |
| Visualforce | MyDomainName--PackageName .trailblaze.vf.force.com ¹ |

¹ If your installed package is unmanaged, the package name is c

SEE ALSO:

[My Domain](#)

[Partitioned Domains](#)

Plan for a My Domain Change

Whether you change your My Domain to update your brand, to adopt enhanced domains, or to enable partitioned domains, the URLs that Salesforce hosts for your org change. Those changes can have a large impact, and making the required updates can seem like a daunting project. To make the process as smooth as possible for you, your users, and your customers, review the high-level steps, the recommended practices, and how to reduce the impact on your users and customers.

[Understand the My Domain Change Process](#)

Review the high-level process to successfully deploy a change to your My Domain. The change can include a My Domain name change, enhanced domains, or partitioned domains.

[Review Recommended Practices for a My Domain Change](#)

Before you deploy a change to your My Domain, consider configuring a custom domain to serve your sites, and review your My Domain settings. Review recommendations for testing and go-live plans. Understand the steps that you can make only after you deploy a My Domain change, and follow recommendations to minimize disruption during your deployment. After you complete testing, notify users, enable redirection logging, and determine when to disable redirections.

[Prepare for and Schedule a My Domain Change](#)

To prepare for a My Domain change, first gather the key information: the required updates, testing, and participants. Then review the deployment process for a My Domain change, identify your testing environment, and schedule your testing and production deployment.

[Notify Users and Customers About a My Domain Change](#)

A My Domain change can impact users who log in to your Salesforce org, and it can impact external users, such as visitors to your Experience Cloud sites. Review recommendations about communicating to these groups before and after you deploy the change.

[Example My Domain Change Checklists](#)

Review example checklists for a My Domain change, including a project checklist, pre-deployment checklist, and post-deployment checklist.

SEE ALSO:

[My Domain](#)

Understand the My Domain Change Process

Review the high-level process to successfully deploy a change to your My Domain. The change can include a My Domain name change, enhanced domains, or partitioned domains.

Here's the step-by-step process to enable, test, and deploy a change to your My Domain.

1. Review the [recommended practices](#) for a My Domain change.
2. [Prepare for and schedule](#) your change.
3. Review the [example checklists](#).
4. Prepare to test in a sandbox.
 - a. Follow the [recommended practices](#) before a My Domain change.
 - b. Save the [change to your My Domain details](#) in the sandbox.
 - c. [Preserve login access](#) for your sandbox.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

- d. [Update](#) your sandbox with changes that can be made before deployment.
5. Test in a sandbox.
 - a. [Deploy](#) the change in your sandbox.
 - b. [Update authentication](#) for your sandbox.
 - c. [Update](#) your sandbox with changes that can only be made after you deploy the My Domain change.
 - d. [Test](#) in your sandbox.
 - e. Follow the [recommended practices](#) after a My Domain change.
 6. Prepare to update production.
 - a. Follow the [recommended practices](#) before a My Domain change.
 - b. [Notify](#) users and customers.
 - c. Save the [change to your My Domain details](#) in production.
 - d. [Preserve login access](#) to production.
 - e. [Update](#) production with changes that can be made before deployment.
 7. Deploy and test in production.
 - a. [Deploy](#) the change in production.
 - b. [Update authentication](#) in production.
 - c. [Update](#) production with changes that can be made only after you deploy the My Domain change.
 - d. [Test](#) in production.
 - e. Follow the [recommended practices](#) after a My Domain change.

SEE ALSO:

[My Domain](#)

[Plan for a My Domain Change](#)

Review Recommended Practices for a My Domain Change

Before you deploy a change to your My Domain, consider configuring a custom domain to serve your sites, and review your My Domain settings. Review recommendations for testing and go-live plans. Understand the steps that you can make only after you deploy a My Domain change, and follow recommendations to minimize disruption during your deployment. After you complete testing, notify users, enable redirection logging, and determine when to disable redirections.

Recommended Steps Before a My Domain Change

- **Preserve Access**—When your My Domain login URL or site URL changes, authentication methods such as single sign-on (SSO) and multi-factor authentication (MFA) can stop working. Before you deploy a change to your My Domain, preserve login access for your admins and users.

 **Important:** If you don't follow this guidance before you deploy a change to your My Domain login URL, you can be locked out of your Salesforce org.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

- Confirm that Your My Domain Name Reflects Your Brand—With enhanced domains, all the URLs that Salesforce hosts for your org include your My Domain name, including the system-managed Experience Cloud sites and Salesforce Sites URLs. If your change includes deploying enhanced domains, verify that your My Domain name reflects your external brand. If not, you can rename your My Domain as part of your My Domain change.



Note: If you use a custom domain such as `https://www.example.com`, your system-managed site URLs aren't visible to your customers.

- Provision Early—To deploy your changes on your schedule, save your desired My Domain change at least 1 day before your scheduled deployment.

After you save a change to your My Domain, Salesforce then provisions the domains. In other words, we get the new My Domain URLs ready for activation. The provisioning process usually finishes in a few minutes, but it can take up to 24 hours. Issues with provisioning are rare, but sometimes they require that you stop the process and save your My Domain change again, which restarts the process.

When the provisioning process is complete, the admin who requested the change receives an email. You can leave your new My Domain in a provisioned status as long as you need. Or, if you choose not to deploy the new Domain, you can cancel the change.

Most importantly, until you deploy your My Domain, user connections are unaffected. If a user visits the new My Domain login URL, they're redirected to the original My Domain login URL. Otherwise, no one can access the new domains.

- Understand Redirections After a My Domain Change and Disable Redirections During Testing—Each time that you deploy a change to your My Domain details, Salesforce redirects your previous My Domain hostnames to the hostnames for your current My Domain unless you disable those redirects. However, if you change your My Domain more than one time, only the last set of My Domain URLs for your org are redirected. Before you deploy a My Domain change, consider the impact on any existing My Domain URL redirections. To see if redirects are in place for a previous My Domain, check the Redirections section of the My Domain page.

My Domain URL redirections help prevent disruption, but they're not intended as a permanent solution. Not all services work well with redirections, and a redirection adds a step to the process of loading the final web page. When you deploy a new My Domain, we highly recommend that you disable redirections during testing and update all references to your old URLs.

For more information on redirections, the settings that control them, and how to log My Domain hostname redirections, see [My Domain Redirections](#).

- Create an inventory of your hard-coded Salesforce org URLs—With a hard-coded URL, the URL exists in plain text in your code. Those URLs require a manual update when the URL changes, such as with a My Domain change or an org migration. For this reason, Salesforce recommends that you use relative and dynamically created URLs instead of hard-coded URLs whenever possible.

The first step to addressing hard-coded links is to find where they exist in your Salesforce orgs. An inventory can help you complete the required updates to your org and include the relevant functionality in your testing.

To search your Salesforce code, download the metadata for each of your Salesforce orgs via a tool such as [Salesforce CLI](#). Then use a code editor such as Microsoft Visual Studio to search for URLs that belong to the org in which you plan to change the My Domain. To determine what to search for, you can use your instanced URL and reference the [My Domain URL formats](#).

Because of the time it can require, we recommend that you create the inventory early in the My Domain change process. We also recommend that your inventory identifies the URLs that point to a different Salesforce org.

- Computer-Telephony Integrations (CTIs), such as Open CTI and Service Cloud Voice: Engage with Telephony Providers—When you deploy enhanced domains or deploy a My Domain name change, the URLs used in your Open CTI or Service Cloud Voice configuration change.

If you use Open CTI for integrations such as Salesforce Call Center and Click to Dial, work with your telephony provider to add your new URLs to the telephony provider's allowlists. Also review your configuration for any hard-coded references to your Salesforce URLs. Whenever possible, update those hard-coded references to relative URLs instead.

If you use Service Cloud Voice with Amazon Connect or Service Cloud Voice with Partner Telephony from Amazon Connect, no action is required. Salesforce updates your configuration for you when you deploy your new My Domain.

If you use Service Cloud Voice with Partner Telephony, connect with your telephony provider. Add your new URLs to their allowlist and coordinate with your provider to update your configuration with your new URLs after you deploy the change.

For more information, see [Update Your Org for My Domain Changes](#).

- Upgrade Mobile Publisher for Experience Cloud Apps—If you configured a Mobile Publisher for Experience Cloud app that uses your .force.com Experience Cloud site URL, before you enable and deploy enhanced domains in production, upgrade to Mobile Publisher version 10.0 or later. For instructions, see [Mobile Publisher for Experience Cloud Apps and Enhanced Domains](#)

If you use a custom domain such as `https://www.example.com` to host your Experience Cloud site and use that custom domain for your Mobile Publisher app, this restriction doesn't apply. Also, this restriction doesn't apply to Mobile Publisher for Lightning apps.

- Review Your My Domain Configuration—A My Domain change is a great time to review your existing configuration, record it for testing and post-deployment verification, and make any changes. For example, on your My Domain login page, update the branding or add the option to log in via an identity provider. To review the available configuration options, see [Configure My Domain Settings](#) and [My Domain Redirections](#).
- Document Your Current Authentication Configuration—If your My Domain change updates your My Domain login URL, Experience Cloud sites URL, or Salesforce Sites URL, we recommend that you document your existing settings before you deploy your My Domain change. This snapshot is valuable reference for your rollback plan. For more information about the settings to capture, see [Determine the Required Authentication Updates After a My Domain Change](#).
- Replace Login References with Dynamically Created Hostnames—For stability and an extra layer of security, we recommend that you use your My Domain login URL to log in to Salesforce with code. To insulate these references against future My Domain changes, use Apex to retrieve the URL. To get the hostname of your My Domain login URL in Apex, use the `getOrgMyDomainHostname()` method of the `System.DomainCreator` class. If you use the system-managed hostname to log in to your Experience Cloud site, use the `getExperienceCloudSitesHostname()` method of the `System.DomainCreator` class to get that hostname.

You can use dynamically created hostnames before you deploy your My Domain change. With dynamically created hostnames, any change to the corresponding system-managed URL doesn't affect the related code. This approach reduces your post-deployment effort.

For more information, see [Log In to Salesforce with Code](#) in Salesforce Help and [DomainCreator Class](#) in the *Apex Developer Guide*.

- Consider a Custom Domain to Serve Your Sites—Custom domains allow you to use a domain that you own, such as `https://www.example.com`, to serve your Experience Cloud sites and Salesforce Sites. Although your Salesforce org provides the content, the site is served on your custom domain, providing a clear branded experience for your users. For this reason, Salesforce recommends that you serve your sites on a custom domain.

If you're considering a custom domain, we recommend that you set up the custom domain before any pending My Domain changes, if possible. Even if the system-managed site URL changes, your customers continue to use the custom domain. That stability reduces the number of updates required after a My Domain change. For example, if you reference your site URL in marketing materials, emails, social media pages, and templates, the custom domain remains valid.

For more information, see [Custom Domains](#).

- Consider Verifying User Addresses—A change to your My Domain login URL is a great time to verify your users as part of rolling out the new login URL. Use async email verification to send email messages to internal and external users to ensure that they're registered with a valid email address that they own. Async email messages contain a verification link (URL). You can also brand the verification email messages by customizing the email template.

For more information, see in [Verify Email Addresses with Async Email](#).

Understand When to Make Updates to Your Org

To create your test and go-live plan, review how to [update your org for a My Domain change](#) and the [example checklists](#) for a My Domain change.

Not all steps apply to every org. When you create your plan, remove the inapplicable steps for your My Domain change. Then prioritize the updates to make after you deploy your My Domain change. For example, authentication and allowlists are essential to complete before the bulk of users start testing.

To reduce downtime in production, identify which updates you can make before you deploy your My Domain change. Then make as many of those updates as possible in production before you deploy the change.

To help you estimate the amount of time needed for production deployment, note the updates that require the new My Domain URLs, and include the updates in your go-live plan.

Test Plan Recommendations

Regardless of whether you have a small or large team for testing, a test plan helps ensure that you cover the required areas of testing.

Here are some recommendations for a My Domain change test plan.

- Test My Domain changes in a sandbox before you update production. You can't test in production without impacting users. After you deploy a My Domain change, it immediately applies to all users and third parties that access your org.
- Prioritize the areas to test. If you have automated tests, run those tests before you start end-user testing. Focus on the biggest impact to your business and the areas for which issue resolution can take the longest. For example, some customers test public-facing sites and revenue-generating functionality first. Or to provide more time for troubleshooting while your testers are engaged, you can prioritize complex customizations. And because resolving issues with package-delivered functionality often requires working with the package developer, test important package features early.
- If you installed packages from [AppExchange](#), include the package-delivered functionality and components in your testing. Focus on components with links. For example, a package-delivered Visualforce page can contain links to your sites, content, or other Visualforce pages. To help triage any issues, we recommend that you note your installed packages and the corresponding functionality in your test plan.

In most cases, you can't edit those package-delivered components. And if you can update one of those components, a future package update can overwrite your changes.

We recommend that AppExchange package developers use relative paths to build any links. If they follow that approach, updated links work after a My Domain change, such as enabling enhanced domains. However, not all package developers follow that recommendation. If you find an issue with components or functionality delivered by a package, remediation can require an updated version of the package. For that reason, we recommend that you test package-delivered functionality early in your testing and that you build time into your overall project for package remediation.

- Whenever possible, provide testers with clear instructions on how to test each feature. If your testers are experienced users who are familiar with all the functionality, it can be unnecessary to spell out each step but it's always helpful to include the expected results.
- Determine the differences in testing in your sandbox versus go-live testing in production. We recommend testing thoroughly in your sandbox. However, due to the assumption that major issues were discovered during sandbox testing, production testing is often less detailed. Decide whether your approach to testing requires two versions of your test plan.

Go-Live Plan Recommendations

A go-live plan ensures that you complete the essential steps when you deploy the change in production.

Here are some recommendations for a My Domain change go-live plan.

- Include steps for provisioning the change and verifying that the change is ready to be deployed.

- Many of these changes, such as updating allowlists and hard-coded URLs, can be made in production before you deploy your new My Domain. To reduce downtime in production, make as many of these changes before you go live as possible.
- Detail any steps that you can only perform after the My Domain change is deployed. Make all other changes before the production deployment window.
- Clarify owners and the proposed timing for each step with all participants.
- Schedule a maintenance event for any impacted public-facing sites.
- As part of the final go-live preparation, confirm the availability and contact details for all participants.
- Include relevant notifications for users and customers in your plan.
- To minimize the impact on your users and customers, deploy your new My Domain when your org receives minimal traffic, such as during the weekend.
- Put mechanisms in place to make public-facing sites available as soon as the related testing is complete.

For an example of the high-level steps, see the Prepare to Update Production, Update Production, and Post-Deployment Adoption sections of the [example My Domain Change project checklist](#). For example steps to perform after you deploy your My Domain change, see the example checklists for [pre-deployment](#) and [post-deployment](#) task example checklists.

Post-Deployment Recommendations

After you deploy a My Domain change, Salesforce redirects your previous hostnames. Some of those redirections stop in Winter '25, starting in August 2024 for sandboxes. To help your users update their outdated bookmarks and links, let them know about the new URL before they're redirected. Enable the My Domain option **Notify users before redirecting to the current My Domain URL**. See [Manage My Domain Redirections](#).

If you enabled and deployed enhanced domains, also review the hostname redirections that stop in Winter '25 and test for the potential impact of that change. For more information, see [Prepare for the End of Redirections for Non-Enhanced Domains](#).

To detect visits of your old hostnames, we recommend that you enable hostname redirection logging. Then, to collect hostname redirection logs for multiple days, schedule a daily query of the Hostname Redirects event type via REST API. For example, you can configure a cron job in Unix or a scheduled task in Windows to run the query. For more information, see [Log My Domain Hostname Redirections](#) in Salesforce Help and the [Hostname Redirects Event Type](#) in Object Reference for the Salesforce Platform.

Consider whether to disable all previous redirections. For example, if your brand changed, determine whether you want users to be able to access your Salesforce org or sites via references to your previous My Domain. For more information on redirections, see [My Domain Redirections](#). If you choose to remove redirections for your old hostnames, treat it as a second My Domain change for testing and communications.

SEE ALSO:

[My Domain](#)

[Plan for a My Domain Change](#)

Prepare for and Schedule a My Domain Change

To prepare for a My Domain change, first gather the key information: the required updates, testing, and participants. Then review the deployment process for a My Domain change, identify your testing environment, and schedule your testing and production deployment.

Determine the Scope

| Task | Details |
|--|--|
| Learn about enhanced domains | <p>If your My Domain change includes enhanced domains, review Enhanced Domains in Salesforce Help and the considerations for enhanced domains. You can also watch the enhanced domains video.</p> <p>To get the latest updates and ask questions about this feature, join the My Domain and Enhanced Domains Trailblazer Community group.</p> |
| Review the My Domain provisioning and deployment process | <p>When you save a change to your My Domain name, Salesforce provisions the new URLs before you can deploy them to your users. To learn about how each step of the process impacts your users' access to Salesforce and why it's important to test these changes in a sandbox, review the process.</p> |
| Determine the hostnames that change | <p>Review the My Domain URL formats and determine which of those hostnames your My Domain change updates. If your project involves renaming your My Domain, all the hostnames in those lists change. If you plan to enable and deploy enhanced domains, review the changes specific to that deployment. And if you plan to enable partitioned domains in a non-production org, review the list of hostnames that contain the partition name after the change.</p> |
| Note whether your login URLs change | <p>If your My Domain login URL or site URL changes, authentication updates are required. Determine whether these changes apply to your My Domain change. Then note the authentication updates required and any third parties involved with those updates. For details, see Determine the Required Authentication Updates After a My Domain Change.</p> |
| Create an inventory of hard-coded Salesforce org URLs | <p>If your URLs change, some steps are required before and after you deploy your My Domain change. Search all your Salesforce orgs for hard-coded URLs that point to the Salesforce org where you're making the My Domain change. Create an inventory so that you can address these URLs before or after you deploy your My Domain change.</p> <p>To search your Salesforce code, download the metadata for each of your Salesforce orgs via a tool such as Salesforce CLI. Then use a code editor such as Microsoft Visual Studio to search for URLs for the org in which you plan to change the My Domain.</p> |
| Identify the features that require an update | <p>For a list of items to update before and after your My Domain change, see Update Your Org for My Domain Changes in Salesforce Help. However, you probably don't use every feature on the list. Identify the updates to make as part of your testing and deployment process. Optionally, you can use the</p> |

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

| Task | Details |
|--|--|
| | example pre-deployment and post deployment task checklists to track the items to update and test. |
| Review recommended practices and identify any additional changes | Salesforce recommends several steps before and after you deploy a My Domain. Determine which recommendations to adopt, and include any relevant steps in your testing and go-live plans. Also factor those steps into your project timelines. For example, if you decide to set up a custom domain to serve your sites, include the time required for that project in your overall project timeline. |

Determine Your Project Participants

| Task | Details |
|--|---|
| Identify participants for the required updates | <p>Now that you know which of your features are impacted, determine who can make the required changes. For example, if your My Domain change requires an update to your domain allowlists, identify who can make that update.</p> <p>Review your integrations and external applications, then determine the involvement and support required from each third party. For example, if your My Domain change requires updating authentication settings, connect with your identity provider (IdP).</p> |
| Identify testers | Use the list of impacted features and your test plan to identify testers. If possible, include knowledgeable end users in your testing, especially for key features. Many tasks in Salesforce can be performed in multiple ways. These users can uncover issues that automated tests can miss. |
| Identify communication owners | Using your communication plan, identify the owners for each communication in your project participant list. |
| Identify go-live participants | Use your go-live plan to determine participants for that event. In addition to people assigned specific tasks, identify anyone required to resolve potential issues discovered during testing. For example, if your custom domain serves your Experience Cloud site, arrange for coverage with the DNS provider and any external hosting providers. |
| Collect contact information | Collect contact information for all project participants. For anyone involved in updating production, collect phone numbers and backup contacts. If you plan to publish a contact sheet for the go-live in production, verify whether the go-live participants are comfortable sharing their contact information with the group. |

Develop Testing, Communication, and Go-Live Plans

| Task | Details |
|--|--|
| Identify any features that automated tests cover | Review any automated tests that you plan to run as part of your verification. Identify features that are impacted by the My Domain change that are covered by these tests. This information can help you prioritize your testing. |
| Create a test plan | Regardless of whether you have a small or large team for testing, a test plan helps ensure that you cover the required areas of testing. For more recommendations on test plans, see Review Recommended Practices for a My Domain Change in Salesforce Help. |

| Task | Details |
|--|---|
| Determine how to capture testing results | <p>Provide a standard method for reporting issues discovered during testing. As you resolve issues, note the changes that are made in the sandbox. You can use that list to update production.</p> <p>Some items that you uncover can only be performed after the change is deployed and your new My Domain URLs are available. Include these items in a checklist for the tasks to perform after you deploy in production.</p> |
| Develop a communication plan | <p>A My Domain change can impact users who log in to your Salesforce org and external users, such as visitors to your Experience Cloud sites. As part of your planning, develop a communication plan, and identify the owners for each communication. For more information on recommended communications, see Notify Users and Customers About a My Domain Change in Salesforce Help.</p> <p>After you identify the owners, confirm the lead time required for each communication method. As part of your plan, specify the conditions required before each communication is sent and methods for the owners to get updates on the status of the project.</p> |
| Create a go-live plan | <p>A go-live plan ensures that you complete the essential steps when you deploy the change in production. For more recommendations on a go-live plan, see Review Recommended Practices for a My Domain Change in Salesforce Help.</p> |
| Develop a rollback plan | <p>The best deployment plans include contingency planning. If you discover a high-impact issue that can't be resolved quickly during your go live, you can restore your original My Domain state. Define a plan for rolling back to the previous state.</p> <p>To roll back a deployed My Domain change, typically you provision and deploy a change with your previous My Domain details. In the rollback plan, include reversing the changes made after you deployed the My Domain change and testing again.</p> <p>Because reversing a deployed My Domain change involves deploying another My Domain change, it can impact existing redirections. For more information, see My Domain Redirections.</p> |

Schedule Your My Domain Change

| Task | Details |
|--|--|
| Identify or create a sandbox for testing | <p>Decide the sandbox or sandboxes to use when you test the My Domain change. Confirm when the sandboxes are available, and identify any steps and lead time required to grant access to your testers.</p> <p>For more information on sandboxes, see Sandboxes: Staging Environments for Customizing and Testing in Salesforce Help and the Set Up a Sandbox in Your Salesforce Org unit in Trailhead.</p> <p>You can't test enabling partitioned domains in a sandbox. If you have multiple orgs of the same non-production type, you can test partitioned domains before enabling them in other orgs of the same type. For example, you can enable partitioned domains in a Developer Edition org that you use less often before you enable the feature in your primary Developer Edition org.</p> |
| Determine your target project dates and dependencies | <p>To determine your target dates, discuss the project with stakeholders. If your My Domain change requires the completion of another project, work closely with the owner of that project to align the dates. If other projects require the new My Domain URLs, discuss their targeted completion date, then align the project dates and expectations.</p> |

| Task | Details |
|--|---|
| | If your My Domain change includes enabling and deploying enhanced domains, that feature is enforced in Winter '24. To verify when enhanced domains are deployed or required in your org, you can find that information on the My Domain Setup page. To find the specific date that you get a release, go to Trust Status , search for your My Domain name, and select your Salesforce instance. Then select the Maintenance tab. For more information, see Get Your Org Status and Upcoming Maintenance Dates with My Domain in Salesforce Help. |
| Choose your testing and deployment windows | Identify any other projects planned or in flight during your planned project timeline, which Salesforce sandboxes those projects plan to use, and any overlapping feature changes. Given that project information, plus your project scope and participants, coordinate with your participants to determine the timeline for deploying the My Domain change in a sandbox, testing, and capturing test results.

Estimate the amount of time required to resolve any issues that arise, and then schedule a target deployment window for production. To minimize the impact on your users and customers, we recommend that you deploy your new My Domain when your org receives minimal traffic, such as during the weekend. |
| Finalize and share your schedule | After collecting input from all participants, share and confirm the timeline and the primary points of contact for participants and stakeholders. |

SEE ALSO:

[My Domain](#)[Plan for a My Domain Change](#)

Notify Users and Customers About a My Domain Change

A My Domain change can impact users who log in to your Salesforce org, and it can impact external users, such as visitors to your Experience Cloud sites. Review recommendations about communicating to these groups before and after you deploy the change.

In this topic, we refer to end users, customers, and partners. Let's clarify the definition of each group.

- End users—Users who log in to your Salesforce org. For example, sales reps, account executives, support representatives, and admins. When possible, include some of these users in your testing.
- Customers—External users who access your Salesforce org data through external-facing sites and functionality. For example, users who visit your Experience Cloud site to shop for your products, to search for job postings at your company, or to search an externally exposed inventory. Customers can be authenticated or unauthenticated. In other words, some guests log in to your site, and some access the site without logging in.
- Partners—External users or companies that interface with your Salesforce org's data. Their interaction can occur through APIs, interfaces, or apps. For example, you can choose to allow a partner to view your Contact data so that they can scrub the address data for accuracy. Or you can allow an external system to provide sales leads.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

Before Your My Domain Change

A change to your My Domain name can impact end users, customers, and partners. To keep your business running smoothly on Salesforce, notify these groups about the change in advance.

When your Salesforce org URLs change, login processes, authentication methods, and commonly visited pages can change. A new URL can require end users and customers to update their bookmarks. If your site URLs change, a marketing or communication campaign can help customers transition to the new site. To keep all the existing functionality working, give your partners plenty of notice and include them in your testing.

End users—Here are the key points to communicate to your end users before you deploy My Domain change.

- Key logistics such as the target time frame for the change, when you expect to complete testing, and the notification process for completion.
- The visible changes. For example, login page or login URL changes and URL changes.
- Anyone logged in to Salesforce when the My Domain change is deployed can be logged out. If a user is logged out, they can log back in again.
- Connections to Salesforce are reset when you deploy the My Domain change. This includes features delivered by managed packages that log in to Salesforce in the background. Notify users that features that connect to Salesforce can stop working, and that they can see prompts to reconnect. If possible, include the known features that require the user to reconnect or reauthenticate.
- Instruct admins to verify that they can log in without authentication features such as single sign-on (SSO) or security keys before the change. For example, they can authenticate via a username and password with a second factor of Salesforce Authenticator.
- If your My Domain login URL or site URL changes, inform users that they can re-register their built-in authenticator or security key when they log in after the change. And recommend that users register or verify a back-up authentication method, such as Salesforce Authenticator or a third-party authenticator before the change. For more information, see [Preserve Login Access During a My Domain Login URL Change](#) in Salesforce Help.
- Instruct your end users to prepare to update their bookmarks for any changed URLs.
- Tell your users to update all bookmarks listed on their Chatter groups.
- Highlight any other company-specific steps to take after the change. For example, if you added Google to the My Domain login page as an identity provider, provide instructions or guidance on how to use that authentication method.
- How to report any issues they encounter after go live.

Customers—If your My Domain change impacts public-facing sites, plan your communications early. If your brand is changing, incorporate the new URLs into your marketing campaign for the new brand. Otherwise, let customers know about the change and encourage them to update any bookmarks.

If your customers log in to your site as authenticated users, determine whether it impacts their login method, and provide these users with post-deployment instructions. For example, notify them about a requirement to log in again after a certain date. To help customers who contact your company with questions after the change, share these instructions with your support team.

Partners—When you [determine the scope and participants for your My Domain change](#), you review all functionality, including integrations and applications that require support from third parties. Let them know about the pending My Domain change as soon as possible, and include them in planning. Identify the key contacts at each vendor or third party, then provide updates on the progress of the project and testing. Clearly communicate the assistance that you require, and confirm key dates such as the go-live weekend and required participation. Also let them know how to contact you with any issues that they uncover during testing or post-deployment.

After Your My Domain Change

Consider providing more updates to each group after the My Domain change.

End users—After you deploy the change, we recommend that you include key details to help your users log in and adjust to the new URLs.

- Remind users to re-register any built-in authenticators and security keys when they log in after the change.
- Enable a message during My Domain redirections that provides the user with the new URL. See [Manage My Domain Redirections](#).

- Instruct users to refresh their bookmarks. If they visit a bookmark that links to an old URL, they're redirected by default. Instruct them to save their bookmarks again after they're redirected. Tell your users to update any bookmarks listed on their Chatter groups.
- Remind users that their connections to Salesforce were reset, which requires them to reauthenticate. For example, in Salesforce CLI, use `force:org:open` to log in again. If a feature isn't working shortly after the My Domain change, try logging in again. For features delivered by a managed package, they can see additional prompts to log in after the My Domain change.
- Recap any company-specific instructions for the change, such as the option to set up a new identity provider or sharing new URLs with customers.
- Summarize the process for reporting any issues that they encounter.

Customers—Ideally, the transition to your new My Domain URLs is relatively invisible to your customers. Consider celebrating any new branding and reminding customers to update their bookmarks. If the process to log in to your site as an authenticated user changed, repeat the instructions for the new process. To help your support team, provide the answers for any anticipated customer questions.

Partners—After you deploy your My Domain change, thank your partners for their participation in testing and go-live. Remind them that the URLs changed, and remind them about the process to report any issues that they encounter.

SEE ALSO:

[My Domain](#)

[Plan for a My Domain Change](#)

Example My Domain Change Checklists

Review example checklists for a My Domain change, including a project checklist, pre-deployment checklist, and post-deployment checklist.

- ✔ **Note:** To create your own version of these checklists, use the My Domain Change Checklist Templates in Quip (available in [English](#) and [Japanese](#) only).

[Example My Domain Change Project Checklist](#)

The items on this list help with planning, scheduling, and performing a My Domain change.

[Example My Domain Change Pre-Deployment Checklist](#)

The items on this checklist don't require the new My Domain URLs to be accessible.

[Example My Domain Change Post-Deployment Checklist](#)

The items on this checklist require your new My Domain URLs, so you can only complete them after you deploy the new My Domain.

SEE ALSO:

[My Domain](#)

[Plan for a My Domain Change](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Example My Domain Change Project Checklist

The items on this list help with planning, scheduling, and performing a My Domain change.

Each company and configuration is different. Use this checklist as a starter when you develop the plan for your My Domain change. Optionally, to create your own version of this checklist, use the My Domain Change Checklist Templates in Quip (available in [English](#) and [Japanese](#) only). For more information on each of these steps, see [Plan for a My Domain Change](#) in Salesforce Help.

Example My Domain Change Project Checklist

[Prepare for and schedule the change.](#)

- If your project includes deploying enhanced domains, review the [considerations](#) for the feature, and join the [Trailblazer Community group](#).
- Review the My Domain [provisioning and deployment process](#).
- Determine the [hostnames](#) that change.
- Note [whether your login URLs change](#).
- Create an inventory of hard-coded URLs that point to the org where you plan to deploy the My Domain change.
- Identify the features that [require an update](#).
- Review [recommended practices](#), and identify any additional changes.
- Identify participants: update owners, testers, communication owners, and go-live participants.
- Identify any features covered by automated tests.
- Create a test plan.
- Determine how to capture testing results.
- Develop a communication plan.
- Create a go-live plan.
- Develop a rollback plan.
- Identify or create a sandbox for testing.
- Determine your target project dates and dependencies.
- Choose your testing and deployment windows.
- Finalize and share your schedule.

Prepare to test in a sandbox.

- Review the [recommended steps](#) to take before and after you deploy a My Domain change.
- Replace login references with dynamically created hostnames.
- Review and document your current My Domain configuration.
- If your login or site URLs change, document your authentication configuration.
- Configure a [custom domain](#) to serve your sites (optional).
- Share test plans and issue reporting instructions with testers.
- Verify that users can access the sandbox.
- [Preserve login access](#) for your sandbox.
- [Update](#) your sandbox with changes that can be made before you deploy the My Domain change.
- [Save](#) the change to your My Domain details in your sandbox.

Test in a sandbox.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

- [Deploy](#) the change in your sandbox.
- [Update authentication](#) for your sandbox.
- Disable [redirections](#) for testing.
- Run automated tests, if applicable.
- [Update](#) your sandbox with changes that can be made only after you deploy the My Domain change.
- [Test](#) in your sandbox. Use your test plan.
- Record changes made to resolve issues.
- Re-enable [redirections](#) (optional).

Prepare to update production.

- [Notify](#) users and customers.
- Update your go-live plan based on testing results.
- Replace login references with dynamically created hostnames.
- Review and document your current My Domain configuration.
- If your login or site URLs change, document your authentication configuration.
- [Update](#) production with changes that can be made before you deploy the My Domain change. Refer to the list of changes made during testing.
- [Preserve login access](#) access to production.
- [Save](#) the change to your My Domain details in production.

Update production.

- [Deploy](#) the change in production.
- [Update authentication](#) in production.
- [Update](#) production with changes that can be made only after you deploy the My Domain change. Refer to the list of changes made during testing.
- Disable [redirections](#) for testing.
- Run automated tests, if applicable.
- [Test](#) in production. Use your test plan.
- If your brand changed, [update your My Domain login page](#) and [update your Experience Cloud site login page](#).
- Re-enable [redirections](#) (optional).

Post-deployment adoption.

- [Notify](#) users and customers about the change.
- Enable My Domain hostname [redirection logging](#), and schedule a daily query of the Hostname Redirects event type.
- Monitor [hostname redirections](#), and determine when to disable redirections.
- Disable [redirections](#) (optional).
- [Update](#) your org to remove references to your old hostnames.
- If your org was created without enhanced domains, disable [redirections for non-enhanced domains](#).
- If you don't want users to access Salesforce from your old My Domain URLs, [remove](#) your previous My Domain.

SEE ALSO:

[Plan for a My Domain Change](#)

[Example My Domain Change Checklists](#)

Example My Domain Change Pre-Deployment Checklist

The items on this checklist don't require the new My Domain URLs to be accessible.

Each company and configuration is different. Use this checklist as a starter list for updating your org before your My Domain change. For the checklist to complete after you deploy your My Domain change, see [Example My Domain Change Post-Deployment Checklist](#).

Optionally, to create your own version of this checklist, use the My Domain Change Checklist Templates in Quip (available in [English](#) and [Japanese](#) only). For more information on each of these steps, see [Update Your Org for My Domain Changes](#) in Salesforce Help.

Example Pre-Deployment Checklist

- Allowlists—Update your allowlists for any new domains.
- Cross-Org Links and Redirections—Create an inventory and plan to update them after you deploy the new domain.
- Custom Visualforce pages or custom apps—Replace references to the org's instance URL with relative URLs and dynamically generated hostnames. Note any URLs that require a hard-coded reference.
- Einstein Bots—Identify the web pages and sites that use your bots. For each chatbot, review the Permitted Domains field in the chat deployment settings.
- External software that accesses your Salesforce org—Verify that the external software that uses your Salesforce URLs, including site URLs, can process redirections. If the software can't process those redirects, work with the software owner to get that redirection functionality in place, or plan to update your use of the software with your new URLs after you deploy the change.
- Firewalls and Proxy Servers—Update trust settings that filter by hostname. Include all applicable URL formats for your new configuration.
- Hard-coded Salesforce org URLs—Create an inventory. Replace hard-coded Salesforce org URLs with relative URLs and dynamically generated URLs when possible. Note the URLs to update after you deploy the change.
- Identity providers on your Salesforce login page—Note any authentication options available to your users.
- Installed Packages from AppExchange—To get the latest fixes, potentially including fixes for enhanced domains, install the latest version of each package. Note the package providers so that you can report any issues detected.

If the change to your My Domain updates your My Domain login URL, complete these tasks.

- Authentication options such as single sign-on (SSO), authentication providers, and named credentials—Plan to update authentication. Document your existing settings for your rollback plan.
- Knowledge articles served on your *.my.salesforce.com URL—Search for hard-coded references to the knowledge article URLs.
- Lightning Out (beta)—Identify the Visualforce pages, web pages, and other locations that call your Lightning Out app. Identify who can update the markup that's embedded in those pages. Determine whether authenticated users access Lightning Out and whether the connected app for Lightning Out uses your My Domain login URL.
- Open Computer-Telephony Integrations (CTI), such as Salesforce Call Center and Click to Dial—Work with your telephony provider to add your new URLs to their allowlists. Review your configuration for any hard-coded references to your Salesforce URLs. Whenever possible, update these references to relative URLs instead, and note any exceptions.
- Preserve login access for your admins and end users.
- Service Cloud Voice with Partner Telephony—Work with your telephony provider to add your new URLs to their allowlist. Also identify hard-coded connect API URLs and references to the Next generation Omni-Channel engagement URL that ends in *.my.salesforce-scrt.com.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

If the change to your My Domain updates your Visualforce URL, complete these tasks. If the change also updates your My Domain login URL, these pre-deployment tasks are included in that section.

- Open Computer-Telephony Integrations (CTI), such as Salesforce Call Center and Click to Dial—Work with your telephony provider to add your new Visualforce URL to their allowlists. Review your configuration for any hard-coded references to your Visualforce URLs. Whenever possible, update these references to relative URLs instead, and note any exceptions.
- Salesforce Maps—Determine whether you show nearby maps in Salesforce records or on sites.
- Service Cloud Voice with Partner Telephony—Work with your telephony provider to add your new Visualforce URL to their allowlist. Also identify hard-coded references to your Visualforce URL in your configuration. Whenever possible, update these references to relative URLs instead, and note any exceptions.

If the change to your My Domain changes your Experience Cloud sites or Salesforce Sites URL, complete these tasks.

- Authentication options such as single sign-on (SSO), authentication providers, and named credentials—Plan to update authentication. Document your existing settings for your rollback plan.
- Embedded Service Deployment (Chat)—Identify the web pages that include chat and identify who can update the code snippet embedded in those pages.
- Knowledge articles served on your Experience Cloud site URL—Search for hard-coded references to the knowledge article URLs.
- Lightning Out (beta)—Identify the connected apps for Lightning Out that use your Experience Cloud sites URL. Determine whether authenticated users access Lightning Out.
- Identity providers on your site login page—Note any authentication options available to your users.
- A Mobile Publisher for Experience Cloud app that uses your Experience Cloud site login URL—Before you deploy enhanced domains in production, upgrade to Mobile Publisher version 10.0 or later.
- Multi-factor authentication (MFA) for your site—Preserve login access for your admins and end users.

If you have Experience Cloud sites or Salesforce Sites and the My Domain change includes deploying enhanced domains, complete these tasks.

- External integrations—Work with third parties that currently integrate with your `*.force.com` site URL to ensure that they support Server Name Indication (SNI).
- IP restrictions are configured in Salesforce with only IPv4 addresses—Update your IP allowlists or restrictions to allow IPv6 source addresses for authorized users. Review and update the login IP range restrictions for the relevant profiles, including the site's guest user profile.
- Network restrictions that use IP allowlists only—Allowlist your site's domain, serve your site via a custom domain, or plan to disable the Salesforce CDN for your `*.my.site.com` URL after you deploy the My Domain change.
- Trusted domains for inline frames—Review and update the list of trusted domains for clickjack protection. Ensure that `*.my.salesforce.com` is trusted.
- Visualforce pages with embedded Lightning components—For each Experience Cloud site with Visualforce pages that include embedded Lightning components, update the Security & Privacy settings, and add your Lightning Components URL to the Trusted Sites for Scripts.

SEE ALSO:

[Plan for a My Domain Change](#)

[Example My Domain Change Checklists](#)

Example My Domain Change Post-Deployment Checklist

The items on this checklist require your new My Domain URLs, so you can only complete them after you deploy the new My Domain.

Each company and configuration is different. Use this checklist as a starter list for updating your org after you deploy your My Domain change. For the checklist of tasks to perform before you deploy your My Domain change, see [Example My Domain Change Pre-Deployment Checklist](#).

Optionally, to create your own version of this checklist, use the My Domain Change Checklist Templates in Quip (available in [English](#) and [Japanese](#) only). For more information on each of these steps, see [Update Your Org for My Domain Changes](#) in Salesforce Help.

Example Post-Deployment Checklist

- Incomplete pre-deployment tasks—Review the [pre-deployment update checklist](#), and complete any incomplete tasks.
- Changed URLs—To help your users update outdated links and bookmarks, enable a [brief message](#) during the redirection that provides the current URL.
- Cross-Org Links and Redirections—Update references to your old My Domain URLs.
- Chatter—Tell your users to update the bookmarks listed on their Chatter groups.
- Custom Visualforce pages or custom apps—Replace references to the org’s instance URL with your new My Domain URL. Whenever possible, use relative URLs and dynamically generated hostnames.
- Einstein Bots—For each bot, regenerate the deployment code and update it on each web page that uses the bot.
- External software that accesses your Salesforce org—Update the references to your Salesforce URLs within the external software, and log in to Salesforce again.
- Hard-coded references to URLs—Update hard-coded references to your old URLs, including instanced hostnames, such as `na87.salesforce.com`. Ideally, generate the hostname via a dynamic method, such as the `DomainCreator` class in Apex. If you deployed enhanced domains, review the hostname redirections that stop in Winter ’25. If you find any of those hostname formats in your org, update them to the enhanced domain format.
- Installed packages from AppExchange—Verify package functionality. For your end-user communications, note the features that require users to reconnect.
- Pinned certificates—Eliminate (recommended) or update the certificates.
- Firewalls and Proxy Servers—Optionally, remove the hostnames that no longer apply to your org from your trust settings. However, we recommend that you allow those hostnames for redirection until all users and integrations are using your new domains successfully.

If the change to your My Domain updates your My Domain login URL, complete these tasks.

- API Integrations—Update API integrations into your org to use the server endpoint. Download your metadata, and then use a command-line interface to search.
- Branding—If your brand changed, update your login page branding
- Desktop links—Update the desktop link with your new My Domain login URL.
- DevOps Center—Update the named credentials used to authenticate users that access your org through DevOps Center.
- Email templates—Update the login URL for your Salesforce org.
- Enablement Sites (myTrailhead)—If your enablement site’s login URL is your My Domain login URL, contact Salesforce Customer Support to update your Sales Enablement authentication provider.
- Identity providers on your login page—Update your identity providers to use your new login URL.
- Knowledge articles served on your `*.my.salesforce.com` URL—Update hard-coded references to the knowledge article URLs.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

- Lightning Out (beta)—Update connected apps that use your My Domain login URL. Refresh the markup on Visualforce pages, web pages, and other locations that call your Lightning Out app. Generate a new Session ID or authentication token for authenticated connections.
- Messaging for In-App and Web—To update your Messaging for Web configuration with your new URLs, republish your Messaging for Web deployment.
- Multi-factor authentication (MFA) for accessing Salesforce—Update authentication.
- Named credentials—Review the URL field for your named credentials. If a named credential uses your My Domain login URL, update the URL field with your new My Domain login URL. If users access functionality that relies on an updated named credential, instruct them to reauthenticate.
- Marketing Cloud Account Engagement (Pardot) —If your configuration uses the Pardot Connector User, update the login URL that Account Engagement uses.



Warning: When you deploy another My Domain change, existing redirections stop.

- Open Computer-Telephony Integrations (CTIs), such as Salesforce Call Center and Click to Dial—Verify and optionally update your telephony provider's allowlist. Update any hard-coded references to your Salesforce URLs in your configuration.
- A personalized version of the Salesforce mobile app published on the Google Play or Apple App stores—If your personalized version of the Salesforce app uses your My Domain login URL, update your app to use your new login URL.
- Service Cloud Voice with Amazon Connect or Service Cloud Voice with Partner Telephony from Amazon Connect—Optionally, remove your old URL formats from the Amazon Connect allowlist.
- Service Cloud Voice with Partner Telephony—Update any hard-coded references to your Salesforce URLs in your configuration. Optionally, remove your old Salesforce URLs from the telephony provider's allowlist.
- Single sign-on for accessing your org—Update authentication.
- Streaming API—Update to use your new My Domain login URL.
- Third-party connected apps that access your org—Work with the app owners to update the login URLs in their app, including SSO and other authentication methods.
- Zones for Experience Cloud sites (Ideas, Answers, Chatter Answers)—Update the email notification URL.

If the Visualforce URL changed, complete these tasks. If the change also updates your My Domain login URL, these post-deployment tasks are covered in that section.

- Open Computer-Telephony Integrations (CTIs), such as Salesforce Call Center and Click to Dial—Update any hard-coded references to your Visualforce URLs in your configuration. Verify and optionally update your telephony provider's allowlist.
- Salesforce Maps—If you show nearby maps in Salesforce records or on sites, update the corresponding Maps Nearby Map component.
- Service Cloud Voice with Partner Telephony—Verify and optionally update your telephony provider's allowlist.

If the content URL changed, complete these tasks.

- Email and other document templates that use files hosted in Salesforce—Update the embedded content or images. Instruct users to update their local templates. For example, an icon or image hosted in your org and used in email footer templates.
- Enablement Sites (myTrailhead)—Update your modules and trails with your new badge art URLs.
- Web content that uses files hosted in Salesforce—Update the content links. For example, an image used on your website or externally published PDFs.

If your Experience Cloud sites or Salesforce Sites URL changed, complete these tasks.

- Authentication that uses your site URL—Verify your configuration. If your setup uses your site URL, update the configuration.
- Branding—If your brand changed, update the branding for your Experience Cloud site login page.
- Desktop links—Update the desktop links with your new site login URL.
- Email templates—Replace references to your old site URLs with your new site URLs.

- Embedded Service Deployment (Chat)—Regenerate the Embedded Service code snippet. Update the web pages that include chat with the new snippet.
- Enablement Sites (myTrailhead)—If your enablement site's login URL is your Experience Cloud sites URL, contact Salesforce Customer Support to update your Sales Enablement authentication provider.
- External integrations—Update external integrations that reference your sites.
- External links to the site—Update all references to the new site URL.
- Hard-coded references to your site within your sites and custom pages—Update the references to your site URL. Where possible, use relative links or dynamically created hostnames.
- Identity providers on your site login page—Update your identity providers to use your new site URL.
- Knowledge articles served on your Experience Cloud sites URL—Update hard-coded references to the knowledge article URLs.
- Lightning Out (beta)—Update connected apps that use your Experience Cloud login URL. Generate a new Session ID or authentication token for authenticated connections.
- Messaging for In-App and Web—If you use Messaging for Web in an Experience Builder site, update your allowlisted URLs.
- A Mobile Publisher for Experience Cloud app—Update your app to use your new Experience Cloud sites URL.
- Multi-factor authentication for accessing your site—Update authentication.
- Named credentials—Review the URL field for your named credentials. If a named credential uses your site URL, update the URL field with your new site URL. If users access functionality that relies on an updated named credential, instruct them to reauthenticate.
- Single sign-on for accessing your site—Update the configuration.
- Third-party connected apps that access your site—Work with the app owners to update the site URLs in their app, including SSO and other authentication methods.
- Trusted domains for inline frames—Review and update the list of trusted domains for clickjack protection. In particular, ensure that `*.my.salesforce.com` is trusted.

If you have Experience Cloud sites the My Domain change included deploying enhanced domains, complete this task.

- Network restrictions that use IP allowlists only—If users on your network can't access your `.my.site.com` URL, allowlist that domain, disable the Salesforce CDN for that URL, or serve your site via a custom domain.

If a custom domain such as `https://www.example.com` serves your Experience Cloud sites or Salesforce Sites and the sites URL changed, complete these tasks.

- The custom domain uses the HTTPS Option: Use a third-party service or CDN to serve the domain—Update the target hostname used when forwarding requests from your domain's proxy or CDN.
- The custom domain serves the site via a non-Salesforce host or service—Review and update the domain configuration, such as CDN settings and hard-coded references to Salesforce URLs.

SEE ALSO:

[Plan for a My Domain Change](#)

[Example My Domain Change Checklists](#)

Change Your My Domain Details

If you don't like your My Domain or circumstances warrant a change, you can rename it. For example, you can change the name when your company's name or branding changes. In some orgs, the admin can also choose a different domain suffix, enable enhanced domains, and remove instance names from certain My Domain URLs.

We recommend that you test a change to your My Domain details in a sandbox. To review the high-level steps, the recommended practices, and how to reduce the impact on your users and customers, see [Plan for a My Domain Change](#) in Salesforce Help.

1. From Setup, in the Quick Find box, enter *My Domain*, and then select **My Domain**.
2. Under My Domain Details, select **Edit**.
The My Domain Details edit page appears.
3. To change your My Domain, enter your new My Domain or suffix. Your chosen My Domain Login URL is displayed.
 - a. To change your My Domain name, enter a new domain name. To confirm that your new name is available, click **Check Availability**. If your name is already taken, choose a different one.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To edit My Domain settings:

- Customize Application

To define a My Domain name:

- Customize Application
AND
Modify All Data

My Domain Details

Current My Domain URL: **mycompany.my.salesforce.com** with enhanced domains

Before changing your My Domain details, review My Domain Considerations in Salesforce Help.

If you change your My Domain name or suffix, you must deploy your new My Domain.

| | | | |
|--------------------------------------|--|--------------------|--|
| My Domain Name | <input type="text" value="mynewbrand"/> | Check Availability | ✔ Available |
| Domain Suffix | <input type="text" value="Standard (*.my.salesforce.com)"/> | | |
| | <input checked="" type="checkbox"/> Use enhanced domains i | | |
| Your chosen new My Domain URL | mynewbrand.my.salesforce.com with enhanced domains | | |

Avoid entering personal information in your domain name. Instead, enter only public information.

In production and sandbox orgs, your name must contain at least 3 characters and no more than 34 characters. In Developer Edition orgs, your name must contain at least 3 characters and no more than 27 characters. It can include letters, numbers, and hyphens, but you can't start the name with a hyphen.

- b. If other suffixes are available for your org's My Domain, a suffix dropdown list appears. To change your My Domain suffix, select a new suffix.

 **Tip:** Unsure of which suffix to pick? For most orgs, the Standard suffix is the best option.

 **Note:** To avoid potential conflicts between follow-up processes such as CNAME and DNS updates, you can't make a change that requires provisioning for 15 minutes after you change your My Domain name or enable enhanced domains. Changes that require provisioning include changing your My Domain name or suffix, enabling enhanced domains, moving to Salesforce Edge Network, and removing your previous My Domain.

4. If your suffix is Standard, select **Use enhanced domains**.

Enhanced domains were enforced in Winter '24. After enhanced domains are deployed, you can disable this feature. Only a limited number of orgs are using legacy My Domain without enhanced domains.

This feature allows your Salesforce login process and related URLs to meet the latest browser requirements. It also stabilizes your My Domain URL by removing the Salesforce instance, preventing user login disruption when your org moves to another Salesforce instance.

 **Important:** Enhanced domains change URL formats across your org. For more information, see [My Domain URL Format Changes When You Enable Enhanced Domains](#). Before you deploy your updated My Domain in production, test it in a sandbox.

5. Optional: Stabilize your Visualforce, Experience Builder, Site.com Studio, and content file URLs.

a. Select **Stabilize Visualforce, Experience Builder, Site.com Studio, and content file URLs**.

 **Note:** If you disabled **Use enhanced domains**, this option is enabled by default. To revert your URLs to their prior formats before enhanced domains were deployed, if this My Domain setting was previously disabled, deselect **Stabilize Visualforce, Experience Builder, Site.com Studio, and content file URLs**.

To determine whether this setting was disabled before enhanced domains were deployed, check the Setup Audit Trail and find the audit trail action for the deployment of your My Domain with enhanced domains. If you see the action, "Enabled the My Domain setting, Stabilize Visualforce, Experience Builder, Site.com Studio, and content file URLs", immediately before the deployment of enhanced domains, then this My Domain setting was disabled before enhanced domains were deployed.

b. Optional: Select **Include the instance name in Visualforce URLs when third-party cookies are blocked**.

This option only applies to the Standard, Database.com, and Cloudforce suffixes when Visualforce URLs are stabilized without enhanced domains.

Third-party cookie blocking can cause issues loading Visualforce pages with stabilized URLs.

 **Note:** If enhanced domains are enabled, these URLs are stabilized and these settings aren't available. Several browsers and operating systems updated their URL requirements after this option was first made available. Enhanced domains provide the latest standard for stabilizing the URLs that Salesforce hosts for your org.

Unless you disabled enhanced domains in a prior step, these settings apply upon saving, without redeploying your My Domain.

6. Save your changes.

If you changed your My Domain name or suffix, or if you enabled or disabled enhanced domains, Salesforce provisions your My Domain. Those changes take effect after you deploy your new My Domain.

The provisioning process usually finishes in a few minutes, but it can take up to 24 hours. You receive an email when your My Domain is ready to be deployed and tested.

When you change your My Domain details, Salesforce redirects your previous My Domain URLs to your current My Domain. If you change your My Domain more than one time, only the last set of My Domain URLs for your org are redirected. For more information, see [My Domain Redirections](#).

Next Steps:

- Salesforce provisions your updated My Domain URLs. The provisioning process usually finishes in a few minutes, but it can take up to 24 hours. You receive an email when your updated My Domain is ready to be deployed and tested.
- Review the changes to your org's URLs in [My Domain URL Formats](#).
- [Deploy your new My Domain, update your org, and test the changes](#).

SEE ALSO:

[My Domain Considerations](#)

[My Domain URL Formats](#)

[Enhanced Domains](#)

[Disable or Remove Your Previous My Domain](#)

Update Your Org and Test My Domain Changes

Before you deploy a change to your My Domain, work with your users to preserve their login access to your org. To test My Domain changes, deploy the change in a sandbox. If your My Domain login URL or site URL changes, update authentication. Review and make the required updates to support the new domains. Then test access to your org and your functional workflows in Salesforce. After you complete testing in a sandbox, use the same process to update your production org. Finally, update redirection behavior for your old URLs.

 **Note:** Whether you change your My Domain to update your brand or to adopt enhanced domains, the URLs that Salesforce hosts for your org change. To review the high-level steps, the recommended practices, and how to reduce the impact on your users and customers, see [Plan for a My Domain Change](#) in Salesforce Help.

[Preserve Login Access During a My Domain Login URL Change](#)

When your My Domain or site login URL changes, two multi-factor authentication (MFA) verification methods stop working: built-in authenticators and security keys. Without those methods, single sign-on (SSO) can also stop working. To preserve admin access to Salesforce and prevent end-user frustration, verify your backup authentication methods. In preparation for your My Domain change, determine the post-deployment steps to reestablish authentication for your org, including resetting the affected verification methods for your users.

[Deploy My Domain Changes](#)

After you change your My Domain and Salesforce provisions those changes, deploy your new My Domain URLs. Only after you deploy your new My Domain can you test your new URLs. And your users can't use the new My Domain URLs until you deploy the updated My Domain.

[Update Authentication After a My Domain Change](#)

Determine whether your My Domain change requires that you update your authentication settings. Then learn about the authentication settings that can be impacted after a My Domain change and make the required updates. If your My Domain login hostname or sites hostname changed when you deployed a My Domain change, update your authentication settings.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

[Update Your Org for My Domain Changes](#)

When you deploy enhanced domains or another change your My Domain, your Salesforce org's login URL and application URLs change. URLs that are dynamically constructed—for example, URLs generated via the `DomainCreator` Apex class—use the new URLs automatically. However, some Salesforce functionality requires an update to work with your new URLs. Similarly, custom code, your network configuration, and third-party integrations that use the old URLs require updates. To ensure a smooth transition to your new URLs, update references to your old URLs.

[Test My Domain Changes](#)

Follow these guidelines to test My Domain changes and to ensure a smooth transition to the new My Domain URLs.

Preserve Login Access During a My Domain Login URL Change

When your My Domain or site login URL changes, two multi-factor authentication (MFA) verification methods stop working: built-in authenticators and security keys. Without those methods, single sign-on (SSO) can also stop working. To preserve admin access to Salesforce and prevent end-user frustration, verify your backup authentication methods. In preparation for your My Domain change, determine the post-deployment steps to reestablish authentication for your org, including resetting the affected verification methods for your users.

If you make one of these changes, your My Domain login URL changes and authentication methods can fail.

- Renaming your My Domain.
- Changing your My Domain suffix.
- Sandboxes only: deploying enhanced domains.
- Deploying a change that enables or disables partitioned domains in a Developer Edition org, scratch org, patch org, demo org, free org, or Trailhead Playground.

If you make one of these changes, your Experience Cloud site or Salesforce Site URL changes and authentication methods for your site can fail.

- Deploying enhanced domains.
- Renaming your My Domain in an org with enhanced domains.
- Deploying a change that enables or disables partitioned domains in a Developer Edition org, scratch org, patch org, demo org, free org, or Trailhead Playground.

Authentication against your site login URL is affected only if you use the system-managed site URL to authenticate. System-managed site URLs end in `*.my.site.com` for Experience Cloud sites and `*.my.salesforce-sites.com` for Salesforce Sites. If you authenticate via a custom domain, such as `https://www.example.com`, that serves your Experience Cloud site or Salesforce Site, then the corresponding SSO configuration and MFA verification methods are unaffected.

 **Note:** A change to your My Domain login URL or site URL requires updates to your org beyond authentication methods and settings. For details, see [Update Your Org for My Domain Changes](#).

Note Your Configured Authentication Methods and Review Post-Deployment Steps

You can configure your My Domain or site login page to allow users to authenticate through third parties, such as Google. Before you deploy the change to your My Domain, visit the corresponding login pages and note the available options.

We also recommend that you review the Authentication Settings on the My Domain Setup page. Note the selected settings and plan to update the corresponding authentication methods after you deploy your new My Domain. After you deploy the change, verify that the login page settings are correct with the new URL.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

For more information on updating authentication after a My Domain change that affects your login URLs, see [Update Authentication After a My Domain Change](#). When you review this section before you deploy a My Domain change, you can gather the list of updates to make before users and third parties access your updated org.

Instruct Admins to Verify Their Backup Authentication Method

Before you deploy one of these changes that affects your My Domain login URL, make sure that your admins can log in without authentication features such as SSO or security keys. For example, they can authenticate via a username and password, with a second factor of Salesforce Authenticator.

 **Important:** Ensure that at least one admin registers Salesforce Authenticator or a third-party authenticator app as a backup method before you deploy a change to your My Domain login URL. Otherwise the admin can't log in and help reset authentication settings or other users' verification methods after the new My Domain is deployed.

If your admins previously registered Salesforce Authenticator or a third-party authenticator app as a backup method, instruct them to verify that authentication method before you deploy the change.

Help Users Restore Built-In Authenticator and Security Key Verification Methods

When your My Domain login URL or site URL changes, two multi-factor authentication (MFA) verification methods stop working: built-in authenticators and security keys. If any of your users only use these methods to authenticate when they log in to Salesforce, they can't log in after the login URL changes.

 **Tip:** Not sure who in your org has registered built-in authenticators or security keys for MFA logins? Create a custom list view of users or review the Identity Verification Methods report. For more information, see [See How Your Users Verify Their Identity](#). To learn more about built-in authenticators or security keys, see [Verification Methods for Multi-Factor Authentication](#).

Make it easy for these users to restore their authentication methods after the My Domain change.

- Before the scheduled deployment of your My Domain change, instruct affected users to register Salesforce Authenticator or a third-party authenticator app as a backup verification method. These types of verification methods aren't affected by My Domain changes.

This approach allows your users to restore their original verification methods at their convenience. It can reduce support tickets related to logging in to Salesforce after the My Domain change. Also, if a user loses a device or security key, a backup verification method can preserve their access.

For more information, see [Connect Your Salesforce Account to Salesforce Authenticator](#) or [Verify Your Identity with a TOTP Authenticator App](#).

- As part of your communication for the My Domain change, let users know that they can re-register their built-in authenticator or security key when they log in after the change.
- When you make updates to your org after you deploy the My Domain change, disconnect the built-in authenticator and security key verification methods for all users in Setup.

After you disconnect the methods, users can reconfigure the verification methods. If one of the affected users didn't register a backup method before the change, this step is required the first time that they log in to Salesforce with the new login URL.

For more information on that process, see [Disconnect a User's Verification Method](#). You can also disconnect security keys for all users through the `UserManagement.deregisterVerificationMethod()` Apex method.

SEE ALSO:

- [My Domain](#)
- [Update Authentication After a My Domain Change](#)
- [Multi-Factor Authentication](#)
- [Apex Reference Guide: UserManagement.deregisterVerificationMethod\(\)](#)

Deploy My Domain Changes

After you change your My Domain and Salesforce provisions those changes, deploy your new My Domain URLs. Only after you deploy your new My Domain can you test your new URLs. And your users can't use the new My Domain URLs until you deploy the updated My Domain.

! **Important:** When your My Domain login URL or site URL changes, authentication methods such as single sign-on (SSO) and multi-factor authentication (MFA) can stop working. Before you deploy a change to your My Domain, [preserve login access](#) for your admins and users.

Follow these guidelines when you deploy a My Domain change.

- Whether you change your My Domain to update your brand or to adopt enhanced domains, the URLs that Salesforce hosts for your org change. To review the high-level steps, the recommended practices, and how to reduce the impact on your users and customers, see [Plan for a My Domain Change](#) in Salesforce Help.
 - Test My Domain changes in a sandbox before you update production. You can't test in production. After you deploy a My Domain change, it immediately applies to all users and third-parties that access your org.
 - In case you must troubleshoot any issues, we recommend that you deploy your new My Domain when your org receives minimal traffic, such as during the weekend.
 - When you deploy a My Domain change, active user sessions can be terminated. Similarly, any connection to Salesforce can be reset when you deploy the My Domain change. If a feature that connects to Salesforce stops working, the user can reauthenticate. For example, in Salesforce CLI, use [force:org:open](#) to log in again.
 - Before you deploy a My Domain change, including enabling or disabling enhanced domains, consider the impact on any existing My Domain URL redirections. Salesforce only redirects your last set of previous My Domain URLs. For more information, see [Understand Redirections for Previous My Domain Hostnames](#).
1. Return to the My Domain Setup page. From Setup, in the Quick Find box, enter *My Domain*, and then select **My Domain**. If your domain is provisioned and ready to deploy, the My Domain Setup page shows Step 3: Deploy Your New Domain.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To edit My Domain settings:

- Customize Application

To define a My Domain name:

- Customize Application
- AND
- Modify All Data

My Domain Settings [Help for this Page](#)

A My Domain showcases your company's brand and keeps your data more secure by making your Salesforce org's URL customer-specific. A My Domain is also required for many Salesforce features.

Set up a My Domain in three steps:

1. Choose and register a My Domain
2. Salesforce provisions your new domain
3. Deploy your new domain to users

Step 3: Deploy Your New Domain

Your new domain has been provisioned and is ready to be deployed to users.

| | |
|----------------|--|
| Current domain | mycompany.my.salesforce.com with enhanced domains |
| New domain | mynewbrand.my.salesforce.com with enhanced domains |

The current domain and new domain fields show the My Domain login URL. However, Salesforce serves multiple domains for your Salesforce org. For example, if you enabled enhanced domains, the My Domain login URL doesn't change in production, but site, Visualforce, content, and many other URLs change. For more information on the URLs that Salesforce serves for your org and the potential impact, see [My Domain URL Formats](#) for details.

As part of the provisioning process for your new domain, Salesforce performs a cursory check to ensure that you have network access to the new domains. If you don't have the required access, the My Domain page lists the URLs you can't access. Before you can deploy your new domain, resolve these network access issues. The access issues can be temporary, such as connectivity issues stemming from a stale DNS cache. Or they can require updates to your allowlists or network configuration. To deploy your My Domain, revisit the My Domain Setup page after the access issues are resolved.

If the My Domain Setup page shows Step 2: Provisioning in Progress, Salesforce is still provisioning your new domain. The provisioning process usually finishes in a few minutes, but it can take up to 24 hours. You receive an email when the process finishes. If you continue to see the Provisioning in Progress page 24 hours after submitting your My Domain name, you can click **Stop Provisioning** to stop the process. After you stop the process, wait 15 minutes, and then try registering your My Domain name again. Or you can contact Salesforce Customer Support.

2. Optionally, if you renamed your My Domain, update your My Domain settings, such as adding authentication services. For more information, see [Configure My Domain Settings](#).

 **Note:** My Domain settings apply to your org's deployed and provisioned domains.

3. To roll out the new My Domain to your org, click **Deploy New Domain**, and click **OK**.
When you deploy your My Domain, it's activated immediately. You can now set login policies. See [Set the My Domain Login Policy](#).
Before you test the deployed My Domain, update all URL references in your org.
4. To cancel your requested My Domain changes, click **Cancel New Domain**.

 **Note:** To avoid potential conflicts between follow-up processes such as CNAME and DNS updates, you can't make a change that requires provisioning for 15 minutes after you deploy or cancel a new My Domain. Changes that require provisioning include changing your My Domain name or suffix, enabling enhanced domains, removing a previous My Domain name, and moving to Salesforce Edge Network.

Each time that you deploy a change to your My Domain, Salesforce redirects requests from your previous My Domain URLs to your current My Domain. If you don't want those requests to be redirected, see [Disable or Remove Your Previous My Domain](#).

Next steps:

- Review the changes to your org's URLs in [My Domain URL Formats](#).
- [Update your org](#).
- [Test the changes](#).

SEE ALSO:

[My Domain](#)

[Configure My Domain Settings](#)

[Set the My Domain Login Policy](#)

Update Authentication After a My Domain Change

Determine whether your My Domain change requires that you update your authentication settings. Then learn about the authentication settings that can be impacted after a My Domain change and make the required updates. If your My Domain login hostname or sites hostname changed when you deployed a My Domain change, update your authentication settings.

[Determine the Required Authentication Updates After a My Domain Change](#)

If your My Domain login URL or site URL changes, authentication updates are required. Determine whether these changes apply to your My Domain change. Then understand the types of updates required.

[Update Named Credentials After a My Domain Change](#)

To simplify the setup of authenticated callouts, you can use a named credential as the callout endpoint. When your My Domain login URL or site login URL changes, named credentials that use that URL stop working. Because DevOps Center uses named credentials, you can't access DevOps Center environments when the org's My Domain login URL changes. To reestablish the impacted authentication callouts, update the URL field for the affected named credentials.

[Update Your SAML SSO IdP Configuration After a Login or Site URL Change](#)

After you deploy a My Domain change that updates your My Domain login URL or site URL, SAML Single Sign-On (SSO) authentication stops working. To allow your users to use this SSO method again, work with your Identity Provider to update your configuration.

[Update Your Auth Provider or OpenID Connect IdP Configuration After a Login URL Change](#)

After you deploy a My Domain change that updates your My Domain or site login URL, OpenID Connect single sign-on (SSO) authentication stops working. OpenID Connect SSO options include Authentication Providers. To allow your users to use this SSO method again, work with your identity provider (IdP) to update your configuration.

[Update Service Provider Endpoints After a Login or Site URL Change](#)

When Salesforce acts as an Identity Provider, users can log in to the external service provider or relying party with credentials from your Salesforce org. For example, your users log in to a custom app with their Salesforce credentials or their Experience Cloud site credentials. When your My Domain or site login URL changes, authentication methods that rely on that URL stop working. To restore this authentication method for your users, share the updated endpoints with the third-party service providers.

SEE ALSO:

[Update Your Org and Test My Domain Changes](#)

EDITIONS

Available in: both Salesforce Classic (**not available in all orgs**) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Determine the Required Authentication Updates After a My Domain Change

If your My Domain login URL or site URL changes, authentication updates are required. Determine whether these changes apply to your My Domain change. Then understand the types of updates required.

Connections to Salesforce

When you deploy a My Domain change, all connections to Salesforce are reset. Active user sessions are terminated and security tokens are revoked.

After you deploy the My Domain change, users are required to log in to Salesforce again. If a feature that connects to Salesforce stops working, the user can reauthenticate. For example, in Salesforce CLI, use `force.org:open` to log in again. Also, after you deploy a My Domain change, functionality delivered by a managed package can require that you log in again. For example, if you use [Declarative Lookup Rollup Summaries \(DLRS\)](#), access the summary tool after you deploy your My Domain change and reestablish your connection.

We recommend that you notify your users about this behavior before and after a My Domain change. For more information, see [Notify Users and Customers About a My Domain Change](#) in Salesforce Help.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Determine Whether Your Change Requires an Authentication Update

If you make one of these changes, your My Domain login URL changes and authentication methods can fail.

- Renaming your My Domain.
- Changing your My Domain suffix.
- Sandboxes only: enabling enhanced domains.
- Enabling or disabling partitioned domains in a Developer Edition org, scratch org, patch org, demo org, free org, or Trailhead Playground.

If you make one of these changes, your Experience Cloud site or Salesforce Site URL changes and authentication methods for your site can fail.

- Enabling enhanced domains.
- Renaming your My Domain in an org with enhanced domains.
- Enabling or disabling partitioned domains in a Developer Edition org, scratch org, patch org, demo org, free org, or Trailhead Playground.

Authentication against your site login URL is affected only if you use the system-managed site URL to authenticate. System-managed site URLs end in `*.my.site.com` for Experience Cloud sites and `*.my.salesforce-sites.com` for Salesforce Sites. If you authenticate via a custom domain, such as `https://www.example.com`, that serves your Experience Cloud site or Salesforce Site, then the corresponding single sign-on (SSO) configuration and MFA verification methods aren't affected.

 **Note:** A change to your My Domain login URL or site URL requires updates to your org beyond authentication methods and settings. For details, see [Update Your Org for My Domain Changes](#) in Salesforce Help.

Named Credentials

To simplify the setup of authenticated callouts, you can use a named credential as the callout endpoint. The named credential specifies the URL of a callout endpoint and its required authentication parameters.

When your My Domain login URL or site login URL changes, named credentials that use that URL stop working. To reestablish the impacted authentication callouts, update the URL field for the affected named credentials. For more information, see [Update Named Credentials After a My Domain Change](#) in Salesforce Help.

Impacted Authentication Methods

When your My Domain login URL or site URL changes, authentication methods such as SSO and multi-factor authentication (MFA) can stop working.

To preserve access to Salesforce and prevent end-user frustration, verify backup methods and communicate to your users before you deploy the change. For more information, see [Preserve Login Access During a My Domain Login URL Change](#) in Salesforce Help.

When Salesforce acts as the service provider, authentication is delegated via an identity provider (IdP). If your My Domain login URL or site URL changes, work with your IdP to update your configuration to allow these methods to authenticate against the new URL. These changes can only be made after you deploy the change to your My Domain.

| Method | Example | How to Detect Whether This Method Is In Use |
|---|---|--|
| SAML SSO with Salesforce as the Service Provider | Authentication is delegated to a third-party identity provider such as Okta, OneLogin, Azure, or another Salesforce org. | From Setup, in the Quick Find box, enter <i>Single Sign-On</i> , and then select Single Sign-On Settings .
Active records exist in the SAML Single Sign-On Settings table.
If you're not sure whether a given SAML Single-Sign On setting or Auth. Provider record is in use, review your login history . |
| Salesforce acts as the service provider for single sign-on (SSO) via an Authentication Provider or OpenID Connect | Authentication is delegated to a third-party identity provider such as Google, Facebook, or a third party that operates over the OpenID Connect protocol. Or authentication is delegated to a custom authentication provider that supports OAuth 2.0. | From Setup, in the Quick Find box, enter <i>Auth. Providers</i> , and then select Auth. Providers .
Active Auth. Provider records exist that aren't Salesforce Managed. As a reminder, Salesforce Managed Auth. Providers aren't recommended. |

For instructions on how to update your IdP in these cases, see [Update Your SAML SSO IdP Configuration After a Login or Site URL Change](#) and [Update Your Auth Provider or OpenID Connect IdP Configuration After a Login URL Change](#) in Salesforce Help.

When Salesforce acts as the identity provider, users can log in to an external service provider or relying party with credentials from your Salesforce org. With these methods, if your My Domain or site login URL changes, share the updated endpoints with the third-party service providers to allow them to authenticate against the new URL. These changes can only be made after you deploy the change to your My Domain.

| Method | Example | How to Detect Whether This Method Is In Use |
|--|--|--|
| Salesforce as a SAML Identity Provider | Your Salesforce org acts as a SAML identity provider. Users log in to external services such as Google Apps with their Salesforce or site credentials. | From Setup, in the Quick Find box, enter <i>Identity Provider</i> , and then select Identity Provider .
Enable Identity Provider is selected.
To view the history of outbound usage for Salesforce as an identity provider via SAML, use the Identity Provider Event Log . |

| Method | Example | How to Detect Whether This Method Is In Use |
|--|---|---|
| A connected app uses Salesforce as an Identity Provider through OpenID Connect | A custom app is integrated as a connected app with OpenID Connect. Your users can log in to the custom app with their Salesforce or site credentials. | <p>From Setup, in the Quick Find box, enter <i>Apps</i>, and select App Manager.</p> <p>View or edit each app. If Enable OAuth Settings is selected, then third parties can use Salesforce as an identity provider for that app.</p> <p>The Enable OAuth Settings setting only indicates that third parties can use the app. To determine whether the app is in use, note the third-party service represented by the application. Then work with your partners to determine whether they use your Salesforce org as an identity provider or if they reference your My Domain or site login URL for OAuth authentication.</p> |

For instructions on how to update your service provider in these cases, see [Update Service Provider Endpoints After a Login or Site URL Change](#) in Salesforce Help.

Integrated Logins

Before you deploy the change to your My Domain, visit the corresponding login pages and note the available options.

If your users can authenticate with alternate identity providers or a SAML Single Sign-On (SSO) authentication method from your My Domain login page or Experience Cloud site login page, those authentication methods stop working when the page's URL changes and can be removed from the page. To restore these authentication methods:

- For each authentication method, update the corresponding authentication service.
 - For alternate identity providers, such as Google, Facebook, or a third party that operates over the OpenID Connect protocol, see [Update Your Auth Provider or OpenID Connect IdP Configuration After a Login URL Change](#) in Salesforce Help.
 - For SAML Single Sign-On (SSO) authentication methods include Okta, OneLogin, Azure, or another Salesforce org, see [Update Your SAML SSO IdP Configuration After a Login or Site URL Change](#) in Salesforce Help.
- Verify the authentication method on the login page. If necessary, readd authentication providers to your login page.
 - For your org's My Domain login page: [Add an Authentication Provider to Your Org's Login Page](#) in Salesforce Help.
 - For your Experience Cloud site's login page: [Add an Authentication Provider to Your Experience Cloud Site's Login Page](#) in Salesforce Help.

Login Page Configuration

We also recommend that you review the Authentication Settings on the My Domain Setup page and your site login page configuration. After you deploy the change, verify that those settings are correct with the new URL. For more information, see [Customize Your My Domain Login Page with Your Brand, Brand Your Identity Experience](#), and [Manage Salesforce Sites Login and Registration Settings](#) in Salesforce Help.

DevOps Center

If you use DevOps Center, update the named credentials used to access the DevOps Center environment for your org. For more information, see [Update Named Credentials After a My Domain Change](#) in Salesforce Help.

SEE ALSO:

[Update Authentication After a My Domain Change](#)

[Monitor Login History](#)

[Use the Identity Provider Event Log](#)

Update Named Credentials After a My Domain Change

To simplify the setup of authenticated callouts, you can use a named credential as the callout endpoint. When your My Domain login URL or site login URL changes, named credentials that use that URL stop working. Because DevOps Center uses named credentials, you can't access DevOps Center environments when the org's My Domain login URL changes. To reestablish the impacted authentication callouts, update the URL field for the affected named credentials.

1. From Setup, in the Quick Find box, enter *Named Credentials* in the Quick Find box, then select **Named Credentials**.
2. To modify an existing named credential, click **Edit**.
To find the affected named credentials, look for your old My Domain login URL or site login URL in the URL field.

To locate the named credential records that DevOps Center uses to access your org, look for the environment's DevOps Center record ID in the Label field. DevOps Center uses this pattern:

environmentRecordID_projectName_environmentName_sequentialNumber.

3. In the URL field, replace your old login URL with your new login URL.
For example, replace `https://ExperienceCloudSitesSubdomainName.force.com/hr/jobpostings` with `https://MyDomainName.my.site.com/hr/jobpostings`.

Or if you enabled enhanced domains in a sandbox, replace

`https://MyDomainName--SandboxName.my.salesforce.com` with
`https://MyDomainName--SandboxName.sandbox.my.salesforce.com`.

4. Deselect **Start Authentication Flow on Save** and save your changes.
5. Verify your changes.
 - a. Trigger a callout that uses the updated named credential.

For example, use aAnn external service that uses the named credential to access your org through Salesforce Connect. Or access DevOps Center and perform an operation against the environment that uses the named credential.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

USER PERMISSIONS

To view named credentials:

- View Setup and Configuration

To create, edit, or delete named credentials:

- Customize Applications

- b. When prompted, reauthenticate with your credentials for the affected org.

If your authentication fails, double-check the URL and update the named credential record if needed.

The first time a user accesses functionality that uses the updated named credential, the user is prompted to reauthenticate. Include this detail in your communication plan for the My Domain change.

SEE ALSO:

[My Domain](#)

[Configure My Domain Settings](#)

[Set the My Domain Login Policy](#)

Update Your SAML SSO IdP Configuration After a Login or Site URL Change

After you deploy a My Domain change that updates your My Domain login URL or site URL, SAML Single Sign-On (SSO) authentication stops working. To allow your users to use this SSO method again, work with your Identity Provider to update your configuration.

-  **Important:** Before you deploy a change that updates your login URL or you update your authentication settings, make sure that you can access Salesforce after the change. Double-check that at least one admin can log in without authentication features such as SSO, built-in authenticators, or security keys. For more information, see [Preserve Login Access During a My Domain Login URL Change](#).

After you deploy the change that updates your My Domain login URL, work with your Identity Provider (IdP) to update your IdP configuration with the new authentication values.

These steps also apply after your Experience Cloud site URL or Salesforce Site URL changes, but only if you use the system-managed site URL to authenticate. System-managed site URLs end in

`*.my.site.com` for Experience Cloud sites and `*.my.salesforce-sites.com` for Salesforce Sites. If you authenticate via a custom domain, such as `https://www.example.com`, that serves your Experience Cloud site or Salesforce Site, then your SSO configuration is unaffected.

1. In the Quick Find box, enter `Single Sign-On`, and then select **Single Sign-On Settings**.
2. View the details for each entry in the SAML Single Sign-On Settings table.
The updated values are shown in the Endpoints section.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

SAML Single Sign-On Settings

[Back to Single Sign-On Settings](#)

[Edit](#) [Delete](#) [Clone](#) [Download Metadata](#) [SAML Assertion Validator](#)

| | | | |
|--|---|-----------|-------------------------------------|
| Name | My Company Okta SSO | API Name | MyCompany_Okta_SSO |
| SAML Version | 2.0 | | |
| Issuer | https://www.okta.com/e0000000000000000086 | Entity ID | https://mycompany.my.salesforce.com |
| Identity Provider Certificate | EMAILADDRESS=info@okta.com, CN=salesforce, OU=SSOProvider, O=Okta, L=San Francisco, ST=California, C=US
Expiration: 24 Sep 2031 21:14:17 GMT | | |
| Request Signing Certificate | SelfSignedCert_04Aer2022_135919 | | |
| Request Signature Method | RSA-SHA256 | | |
| Assertion Decryption Certificate | Assertion not encrypted | | |
| SAML Identity Type | Federation ID | | |
| SAML Identity Location | Subject | | |
| Service Provider Initiated Request Binding | HTTP POST | | |
| Identity Provider Login URL | https://mycompany.okta.com/app/my_premier_app/e0000000000000000086/sso/saml | | |
| Custom Logout URL | https://mycompany.okta.com | | |
| Custom Error URL | | | |
| Single Logout Enabled | <input type="checkbox"/> | | |

Just-in-time User Provisioning

User Provisioning Enabled

User Provisioning Type Custom SAML JIT with Apex handler

SAML JIT Handler [AlohaSSO_JIT_Handler](#) Execute Handler As [Premier Apps](#)

Endpoints

View SAML endpoints for your org, Experience Cloud sites, or custom domains.

Your Organization

| | |
|--------------------------|--|
| Login URL | https://mycompany.my.salesforce.com?so=00D0000000000000Q9 |
| Logout URL | https://mycompany.my.salesforce.com/services/auth/sp/saml2/logout |
| OAuth 2.0 Token Endpoint | https://mycompany.my.salesforce.com/services/auth2/token?so=00D0000000000000Q9 |

▼ For Communities

Community Name: Design Partnership Workspace

| | |
|------------|--|
| Login URL | https://mycompany.my.site.com/dpwiflogin?so=00D0000000000000Q9 |
| Logout URL | https://mycompany.my.site.com/services/auth2/token?so=00D0000000000000Q9 |

[Edit](#) [Delete](#) [Clone](#) [Download Metadata](#) [SAML Assertion Validator](#)

3. Share the values in these fields with your Identity Provider.

- Assertion Consumer Service (ACS) URL
- Logout URL
- OAuth 2.0 Token Endpoint
- Entity ID

 **Note:** Some Identity Provider configurations don't use every field.

4. After your Identity Provider updates the settings, verify your updated endpoints with the `/.well-known/auth-configuration` URL path.

For example, if your login URL is `https://mycompany.my.salesforce.com`, visit `https://mycompany.my.salesforce.com/.well-known/auth-configuration`.

5. If your configuration includes SAML Single Sign-On (SSO) that is initiated by the service provider, update your authentication configuration settings on the My Domain page.

- a. From Setup, in the Quick Find box, enter *My Domain*, and then select **My Domain**.
- b. In the Authentication Configuration section, click **Edit**.
- c. In the **Authentication Service** field, select the correct record and save your changes.

 **Note:** If you don't know whether the service provider initiates SAML SSO, before you deploy your My Domain change, view the authentication configuration settings on the My Domain page.

6. Verify the authentication method from your login page. If necessary, add authentication providers to your login page again.
 - a. For your org's My Domain login page, see [Add an Authentication Provider to Your Org's Login Page](#) in Salesforce Help.
 - b. For your Experience Cloud site's login page: [Add an Authentication Provider to Your Experience Cloud Site's Login Page](#) in Salesforce Help.

SEE ALSO:

[Update Authentication After a My Domain Change](#)

[SAML SSO with Salesforce as the Service Provider](#)

[Configure Your Experience Cloud Site as a Service Provider or Relying Party](#)

Update Your Auth Provider or OpenID Connect IdP Configuration After a Login URL Change

After you deploy a My Domain change that updates your My Domain or site login URL, OpenID Connect single sign-on (SSO) authentication stops working. OpenID Connect SSO options include Authentication Providers. To allow your users to use this SSO method again, work with your identity provider (IdP) to update your configuration.

-  **Important:** Before you deploy a change that updates your login URL or you update your authentication settings, make sure that you can access Salesforce after the change. Double-check that at least one admin can log in without authentication features such as SSO, built-in authenticators, or security keys. For more information, see [Preserve Login Access During a My Domain Login URL Change](#).

After you deploy the change that updates your My Domain login URL, work with your identity provider to update your IdP configuration with the new authentication values.

These steps also apply after your Experience Cloud site URL or Salesforce Site URL changes, but only if you use the system-managed site URL to authenticate. System-managed site URLs end in `*.my.site.com` for Experience Cloud sites and `*.my.salesforce-sites.com` for Salesforce Sites. If you authenticate via a custom domain, such as `https://www.example.com`, that serves your Experience Cloud site or Salesforce Site, then your SSO configuration isn't affected.

1. In the Quick Find box, enter `Auth. Providers`, and then select **Auth. Providers**.
2. View the details for each Auth. Provider record.

The updated values are shown in the Salesforce Configuration section.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Auth. Provider Detail

[Edit](#)
[Delete](#)
[Clone](#)

| | |
|--|---|
| Auth. Provider ID | 0SO000000000PS |
| Provider Type | Slack |
| Name | Slack Auth Provider |
| URL Suffix | slack_auth |
| Consumer Key | umyegsOp1gmq5AKFrAE6Qm |
| Consumer Secret | Click to reveal |
| Authorize Endpoint URL | |
| Token Endpoint URL | |
| User Info Endpoint URL | |
| Default Scopes | |
| Include Consumer Secret in API Responses | <input checked="" type="checkbox"/> i |
| Custom Error URL | https://internal.mycompany.com/slack_error |
| Custom Logout URL | https://internal.mycompany.com/slack_logout |
| Registration Handler | AuthORegHandler |
| Execute Registration As | Slack User |
| Portal | |
| Icon URL | https://mycompany.my.salesforce.com/cons/slack.png |

Salesforce Configuration

| | |
|-----------------------------------|--|
| Test-Only Initialization URL | https://mycompany.my.salesforce.com/services/auth/test/slack_auth |
| Single Sign-On Initialization URL | https://mycompany.my.salesforce.com/services/auth/sso/slack_auth |
| Existing User Linking URL | https://mycompany.my.salesforce.com/services/auth/link/slack_auth |
| OAuth-Only Initialization URL | https://mycompany.my.salesforce.com/services/auth/oauth/slack_auth |
| Single Logout URL | https://mycompany.my.salesforce.com/services/auth/rp/oldc/logout |

▼ Experience Cloud Sites

Site Name: Design Partnership Workspace

| | |
|-----------------------------------|--|
| Test-Only Initialization URL | https://mycompany.my.site.com/services/auth/test/slack_auth |
| Single Sign-On Initialization URL | https://mycompany.my.site.com/services/auth/sso/slack_auth |
| Existing User Linking URL | https://mycompany.my.site.com/services/auth/link/slack_auth |
| OAuth-Only Initialization URL | https://mycompany.my.site.com/services/auth/oauth/slack_auth |

[Edit](#)
[Delete](#)
[Clone](#)

3. Share the values in these fields with your identity provider.

- Test-Only Initialization URL
- Single Sign-On Initialization URL
- Existing User Linking URL
- OAuth-Only Initialization URL
- Callback URL

 **Note:** Some identity provider configurations don't use every field.

4. After your identity provider updates the settings, verify your updated endpoints with the `/.well-known/auth-configuration` URL path.

For example, if your login URL is `https://mycompany.my.salesforce.com`, visit `https://mycompany.my.salesforce.com/.well-known/auth-configuration`.

 **Note:** If your identity provider updated the values but the changes aren't reflected in Salesforce, disable the authentication provider in the Authentication Configuration section of the My Domain screen, then enable it again. For more information, see [Add Identity Providers to the My Domain Login Page](#) in Salesforce Help.

5. Before you test your new authentication configuration, verify that the value in the Authentication Service field on the My Domain Setup page matches the authentication service record.
If needed, edit your Authentication Configuration settings on the My Domain Setup page. Then in the **Authentication Service** field, select the correct record and save your changes.
6. Verify the authentication method from your login page. If necessary, add authentication providers to your login page again.
 - a. For your org's My Domain login page, see [Add an Authentication Provider to Your Org's Login Page](#) in Salesforce Help.
 - b. For you Experience Cloud site's login page: [Add an Authentication Provider to Your Experience Cloud Site's Login Page](#) in Salesforce Help.

SEE ALSO:

[Update Authentication After a My Domain Change](#)

[Authentication Provider SSO with Salesforce as the Relying Party](#)

[Configure Your Experience Cloud Site as a Service Provider or Relying Party](#)

Update Service Provider Endpoints After a Login or Site URL Change

When Salesforce acts as an Identity Provider, users can log in to the external service provider or relying party with credentials from your Salesforce org. For example, your users log in to a custom app with their Salesforce credentials or their Experience Cloud site credentials. When your My Domain or site login URL changes, authentication methods that rely on that URL stop working. To restore this authentication method for your users, share the updated endpoints with the third-party service providers.

 **Important:** Before you deploy a change that updates your login URL or you update your authentication settings, make sure that you can access Salesforce after the change. Double-check that at least one admin can log in without authentication features such as SSO, built-in authenticators, or security keys. For more information, see [Preserve Login Access During a My Domain Login URL Change](#).

After you deploy the change that updates your My Domain login URL, work with your Identity Provider (IdP) to update your IdP configuration with the new authentication values.

These steps also apply after your Experience Cloud site URL or Salesforce Site URL changes, but only if you use the system-managed site URL to authenticate. System-managed site URLs end in `*.my.site.com` for Experience Cloud sites and `*.my.salesforce-sites.com` for Salesforce Sites. If you authenticate via a custom domain such as `https://www.example.com` that serves your Experience Cloud site or Salesforce Site, then your SSO configuration is unaffected.

1. After you deploy the My Domain change that updates your login or site URL, validate your configuration with the `/.well-known/auth-configuration` endpoint path.

For example, if your My Domain login URL is `https://mycompany.my.salesforce.com`, visit `https://mycompany.my.salesforce.com/.well-known/auth-configuration`. And if your site URL is `https://mycompany.my.site.com`, visit `https://mycompany.my.site.com/.well-known/auth-configuration`.

 **Tip:** Some service providers and relying parties can use this URL to import the required settings.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

2. For each service provider that relies on Salesforce as an Identity Provider, determine whether the connected app uses SAML, OpenID Connect, or OAuth.
3. If the connected app is integrated with SAML, work with the relying party to update these fields.
 - Issuer URL
 - Well-known metadata endpoints
4. If the connected app is integrated with OpenID Connect or OAuth, work with the service provider or relying party to update these fields.
 - OAuth endpoints
 - Audience for JWT Bearer flow
5. After the service provider or relying party updates the required fields, verify the authentication method by accessing the app with the corresponding Salesforce credentials.

SEE ALSO:

[Update Authentication After a My Domain Change](#)

[Salesforce as an Identity Provider](#)

[Configure Your Experience Cloud Site as an Identity Provider or OpenID Provider](#)

Update Your Org for My Domain Changes

When you deploy enhanced domains or another change your My Domain, your Salesforce org's login URL and application URLs change. URLs that are dynamically constructed—for example, URLs generated via the `DomainCreator` Apex class—use the new URLs automatically. However, some Salesforce functionality requires an update to work with your new URLs. Similarly, custom code, your network configuration, and third-party integrations that use the old URLs require updates. To ensure a smooth transition to your new URLs, update references to your old URLs.

 **Note:** For high-level steps and recommended practices for a My Domain change, plus how to reduce the impact on your users and customers, see [Plan for a My Domain Change](#).

Pre-Deployment Tasks

Complete these tasks before you deploy a My Domain change.

| Feature or Configuration | Task |
|----------------------------------|---|
| Allowlists | Review your allowlists, and ensure that they include the required Salesforce domains . |
| Cross-Org Links and Redirections | <p>Create an inventory of links and redirections that take the user from a different Salesforce org to the org in which you plan to change the My Domain. Search across all your Salesforce orgs.</p> <p>For example, a hard-coded link on a Visualforce page in a sandbox takes a user to a production URL, such as a file or another Visualforce page. Or, if you have multiple production orgs and use redirections to route users to the correct org, note the places in your code where those redirections occur.</p> <p>Plan to update these links and redirections after you deploy your My Domain change.</p> |

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

| Feature or Configuration | Task |
|---|---|
| Custom Visualforce pages or custom apps | <p>Replace references to the org's instance URL with relative URLs and dynamically generated hostnames. Note any URLs that require a hard-coded reference.</p> <p>For more information, see Update References to Hard-Coded URLs for Lightning Experience in Salesforce Help and the knowledge article Updating Hard-Coded References.</p> <p>To search your Salesforce code, download the metadata for each of your Salesforce orgs via a tool such as Salesforce CLI. Then use a code editor such as Microsoft Visual Studio to search for URLs that belong to the org in which you plan to change the My Domain.</p> |
| Einstein Bots | <p>Identify the web pages and sites that use your chatbots so that you can update them after you deploy the change.</p> <p>For each bot, review the Permitted Domains field in the chat deployment settings. Optionally, you can update the permitted domains and update your deployment code before you deploy the My Domain change. For more information, see Create Chat Deployments.</p> |
| External software that accesses your Salesforce org | <p>After you deploy a My Domain change, Salesforce redirects your previous My Domain URLs. In some cases, external software calls can't process the redirection, and the call to the Salesforce URL fails.</p> <p>Before you deploy your My Domain change, verify that the external software that uses your Salesforce URLs, including site URLs, can process redirections. If the software can't process those redirects, work with the software owner to get that redirection functionality in place or plan to update your use of the software with your new URLs after you deploy the change.</p> |
| Firewalls and proxy servers that filter by hostname | <p>Update trust settings to include all applicable URL formats for your new configuration, as described in My Domain URL Formats.</p> |
| Hard-coded Salesforce org URLs | <p>With a hard-coded URL, the URL exists in plain text in your code. Those URLs require a manual update when the URL changes. For this reason, Salesforce recommends that you use relative and dynamically created URLs instead of hard-coded URLs whenever possible.</p> <p>The first step to addressing hard-coded URLs is to find where they exist in your Salesforce orgs. An inventory can help you complete the required updates to your org and include the relevant functionality in your testing.</p> <p>To search your Salesforce code, download the metadata for each of your Salesforce orgs via a tool such as Salesforce CLI. Then use a code editor such as Microsoft Visual Studio to search for URLs that belong to the org in which you plan to change the My Domain. To determine what to search for, you can use your instanced URL and reference the My Domain URL formats.</p> <p>Before you deploy your My Domain name, reduce your post-deployment effort by replacing hard-coded links with relative URLs and dynamically generated URLs. To generate My Domain URLs, use the DomainCreator Class in Apex.</p> <p>Note the hard-coded URLs to update after you deploy your My Domain change.</p> |
| Identity providers on your My Domain login page | <p>Note the authentication options available to your users. For example, the ability to log in to Salesforce with Google credentials. For more information, see Update Authentication After a My Domain Change.</p> |
| Installed packages from AppExchange | <p>To get the latest fixes, including potential fixes for enhanced domains, install the latest version of each package. Note the package providers so that you can report any issues detected during testing. For more information, see Manage Installed Packages in Salesforce Help, and visit AppExchange.</p> |

| Feature or Configuration | Task |
|--------------------------|------|
|--------------------------|------|

| | |
|--------------------|--|
| My Domain settings | Document your configuration on the My Domain Setup page for reference after you deploy the My Domain change. To capture all settings, view or edit each section on the Setup page. |
|--------------------|--|

If the change to your My Domain updates your My Domain login URL, complete these tasks before you deploy the My Domain change. Your My Domain login URL changes when you change your My Domain name or suffix, deploy enhanced domains in a sandbox, or deploy partitioned domains in a non-production org.

| Feature or Configuration | Task |
|--------------------------|------|
|--------------------------|------|

| | |
|--|---|
| Authentication options such as single sign-on (SSO), authentication providers, and named credentials | If any authentication methods use your login URL, plan to update authentication after you deploy the My Domain change. We recommend that you document your existing settings before you deploy your My Domain change. This snapshot of your earlier configuration is a valuable reference for your rollback plan. |
|--|---|

For more information about the settings to capture, see [Determine the Required Authentication Updates After a My Domain Change](#).

| | |
|--|---|
| Knowledge articles served on your <code>*.my.salesforce.com</code> URL | Search for hard-coded references to the knowledge article URLs. |
|--|---|

| | |
|----------------------|---|
| Lightning Out (beta) | Identify the Visualforce pages, web pages, and other locations that call your Lightning Out app. Identify who can update the markup embedded in those pages.

Determine whether authenticated users can access Lightning Out and whether the connected app for Lightning Out uses your My Domain login URL. |
|----------------------|---|

| | |
|--|--|
| Multi-factor authentication (MFA) for logging in to Salesforce | Preserve login access for your admins and end users. |
|--|--|

| | |
|---|---|
| Open Computer-Telephony Integrations (CTIs), such as Salesforce Call Center and Click to Dial | <ul style="list-style-type: none"> Work with your telephony provider to add your new URLs to the telephony provider's allowlists. Review your configuration for any hard-coded references to your URLs. Whenever possible, update these references to relative URLs instead. For examples, see the Knowledge Article Enhanced Domains and Open CTI with Visualforce (Spring '23). If you find any hard-coded references that you can't convert to a relative URL, note them and prepare to update them after you deploy your new My Domain. |
|---|---|

| | |
|---------------------|---|
| Service Cloud Voice | When you enable Service Cloud Voice, Salesforce uses your My Domain URLs to configure single sign-on (SSO) to your telephony provider. The required action depends upon your configuration. <ul style="list-style-type: none"> If you use Service Cloud Voice with Amazon Connect or Service Cloud Voice with Partner Telephony from Amazon Connect, Salesforce updates your configuration, including the Amazon Connect allowlist, when you deploy your new My Domain. No action is required before you deploy the new My Domain. |
|---------------------|---|

| Feature or Configuration | Task |
|--------------------------|------|
|--------------------------|------|

- | | |
|--|--|
| | <ul style="list-style-type: none"> If you use Service Cloud Voice with Partner Telephony, work with your telephony provider to add your new URLs to their allowlist. Also identify hard-coded connect API URLs, allowlists, and references to the Next generation Omni-Channel engagement URL that ends in <code>*.my.salesforce-scr.t.com</code>. With your telephony provider, prepare to update those hard-coded references after you deploy your new My Domain. |
|--|--|

If the change to your My Domain updates your Visualforce URL, complete these tasks before you deploy the My Domain change. Your Visualforce URL changes when you deploy enhanced domains or change your My Domain name.

 **Note:** If the change to your My Domain also updated your My Domain login URL changed, these steps are covered in the corresponding list of pre-deployment tasks in this Help topic.

| Feature or Configuration | Task |
|--------------------------|------|
|--------------------------|------|

| | |
|---|---|
| Open Computer-Telephony Integrations (CTIs), such as Salesforce Call Center and Click to Dial | <ul style="list-style-type: none"> Work with your telephony provider to add your new Visualforce URL to the telephony provider's allowlists. Review your configuration for any hard-coded references to your Visualforce URL. Whenever possible, update these references to relative URLs instead. For examples, see the knowledge article Enhanced Domains and Open CTI with Visualforce (Spring '23). If you find any hard-coded references that you can't convert to a relative URL, note them and prepare to update them after you deploy your new My Domain. |
|---|---|

| | |
|-----------------|---|
| Salesforce Maps | Determine whether you show nearby maps in Salesforce records or on sites. If so, prepare to update the Maps Nearby Map component after you deploy your new My Domain. See Add Nearby Maps to Salesforce Record Pages and Add Nearby Maps to Sites . |
|-----------------|---|

| | |
|---------------------|---|
| Service Cloud Voice | <p>If you use Service Cloud Voice with Partner Telephony, work with your telephony provider to add your new Visualforce URL to their allowlist. Also identify hard-coded references to your Visualforce URL in your configuration. With your telephony provider, prepare to update those hard-coded references after you deploy your new My Domain.</p> <p>If you use Service Cloud Voice with Amazon Connect or Service Cloud Voice with Partner Telephony from Amazon Connect, no action is required. Salesforce updates your configuration when you deploy your new My Domain.</p> |
|---------------------|---|

If your Experience Cloud sites or Salesforce Sites URL change with your My Domain change, complete these tasks before you deploy your My Domain change. Site URLs change when you deploy enhanced domains, change your My Domain name in an org with enhanced domains, or deploy partitioned domains in a non-production org.

| Feature or Configuration | Task |
|--------------------------|------|
|--------------------------|------|

| | |
|---|---|
| Authentication options such as single sign-on, authentication | If any authentication methods use your site URL, plan to update authentication after you deploy the My Domain change. We recommend that you document your existing settings before you deploy |
|---|---|

| Feature or Configuration | Task |
|---|---|
| providers, and named credentials | your My Domain change. This snapshot of your earlier configuration is a valuable reference for your rollback plan.

For more information about the settings to capture, see Determine the Required Authentication Updates After a My Domain Change . |
| Embedded Service Deployment (Chat) | Identify the web pages that include chat and identify who can update the code snippet embedded in those pages. |
| Identity providers on your site login page | Note the authentication options available to your users. For example, the ability to log in to your site with their Salesforce or Google credentials. For more information, see Update Authentication After a My Domain Change . |
| Knowledge articles served on your Experience Cloud site URL | Search for hard-coded references to the knowledge article URLs. |
| A Mobile Publisher for Experience Cloud app | To support redirections of your current My Domain URLs after you deploy the My Domain change, check your Mobile Publisher for Experience Cloud Apps version. If you're running a version lower than 10.0, follow the instructions in the knowledge article Mobile Publisher for Experience Cloud Apps and Enhanced Domains , to upgrade to the latest version before you deploy your My Domain change.

If you use a custom domain such as <code>https://www.example.com</code> to host your Experience Cloud site and use that custom domain for your Mobile Publisher app, this task doesn't apply. Also, this task doesn't apply to Mobile Publisher for Lightning apps. |
| Lightning Out (beta) | Identify the connected apps for Lightning Out that use your Experience Cloud sites URL. Determine whether authenticated users access Lightning Out. |
| Multi-factor authentication for logging in to your site | Preserve login access for your admins and end users. |

If you have Experience Cloud sites or Salesforce Sites and the My Domain change includes enabling enhanced domains, complete these tasks before you deploy the new My Domain.

| Feature or Configuration | Task |
|---|---|
| External integrations | Salesforce uses the Server Name Indication (SNI) protocol to serve the <code>*.my.site.com</code> and <code>*.my.salesforce-sites.com</code> domains. If an integration doesn't support that protocol, the integration can fail. Work with third parties that currently integrate with your <code>*.force.com</code> site URL to ensure that they support SNI. |
| IP restrictions are configured in Salesforce with only IPv4 addresses | After you deploy enhanced domains, your new <code>*.my.site.com</code> Experience Cloud site hostname supports both IPv4 and IPv6. If a profile includes IP restrictions and only IPv4 addresses are allowed, users assigned to that profile can see an error when they access your site that ends in <code>*.my.site.com</code> via IPv6. To prevent that error, update your IP allowlists or restrictions to allow IPv6 source addresses for authorized users. In particular, review and update the login IP range restrictions for the relevant profiles, including the site's guest user profile. For more information on |

| Feature or Configuration | Task |
|--------------------------|------|
|--------------------------|------|

| | |
|--|--|
| | <p>setting IP restrictions in Salesforce, see the knowledge article Network Access, Session Settings, and Profile-based IP restrictions.</p> |
|--|--|

| | |
|--|--|
| | <p>These three IP ranges cover the entire IPv4 and IPv6 internets.</p> |
|--|--|

| | |
|--|---|
| | <pre> :: to ::ffff:ffff:ffff 0.0.0.0 to 255.255.255.255 ::1:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff </pre> |
|--|---|

Network restrictions that use IP allowlists only	<p>When you deploy enhanced domains, your new system-managed Experience Cloud site <code>*.my.site.com</code> domain includes the Experience Cloud Content Delivery Network (CDN), which uses the Salesforce CDN Partner. The IP addresses used by the Salesforce CDN partner, Akamai, aren't published. Therefore, if your network settings include IP allowlisting, users can lose access to your site that uses the Salesforce CDN. For example, if your users log in via a VPN that exclusively uses IP allowlisting, the users on that VPN can't access your site, because it uses an Akamai IP address.</p> <p>To ensure that your users can access your Experience Cloud site on the Salesforce CDN, allowlist your site's domain, or serve your site via a custom domain. For more information, see the knowledge article Access Experience Sites via an IP-Restricted VPN After Enhanced Domains Deployment.</p> <p>If you can't allowlist your domain at the network level or configure a custom domain to serve your site, plan to contact Salesforce Customer Support to disable the Salesforce CDN for your <code>*.my.site.com</code> site URL after you deploy enhanced domains.</p>
--	---

Trusted domains for inline frames	<p>If the Clickjack protection level for your site is Allow framing of site pages on external domains (Good protection), review and update the list of trusted domains. In particular, ensure that <code>*.my.salesforce.com</code> is trusted.</p> <p>For more information, see Enable Clickjack Protection in Experience Cloud Sites and Enable Clickjack Protection in Site.com.</p>
-----------------------------------	--

Visualforce pages with embedded Lightning components	<p>If the Visualforce page is published through an Experience Cloud site, trust your Lightning components URL for scripts on your site. For each site with Visualforce pages that include embedded Lightning components, edit the Security & Privacy settings in Experience Builder and add your Lightning Components URL to the Trusted Sites for Scripts. For example, add <code>https://*.container.force.com</code> or <code>https://*.force.com</code>. For more information, see Where to Allowlist Third-Party Hosts for Experience Builder Sites.</p>
--	---

Post-Deployment Tasks

Complete these tasks after you deploy a My Domain change. Post-deployment tasks require your new My Domain URLs.

Feature or Configuration	Task
--------------------------	------

Incomplete pre-deployment tasks	<p>Review the pre-deployment tasks, and complete any incomplete items.</p>
---------------------------------	--

Feature or Configuration	Task
Allowlists	If you deployed enhanced domains, you can remove the domains that only apply to orgs without enhanced domains from your allowlist. However, we recommend that you keep those domains in your allowlist for redirection until all users and integrations are using your new domains successfully. For the list of required domains and their purposes, see Allow the Required Domains in Salesforce Help.
Changed URLs	With almost every My Domain change, the URLs that Salesforce serves for your org change. Salesforce redirects these URLs by default. To help your users update outdated links and bookmarks, we recommend that you enable a brief message during the redirection that provides the current URL.
Cross-Org Links and Redirections	Update references to your old My Domain URLs in your cross-org links and redirections.
Chatter	Review and update bookmarks and links on Chatter groups that you own.
Custom Visualforce pages or custom apps	Replace hard-coded references to the org's instanced URL, such as <code>https://na170.salesforce.com</code> , or your My Domain login URL with your new My Domain login URL. For more information, see Update References to Hard-Coded URLs for Lightning Experience in Salesforce Help and the knowledge article Updating Hard-Coded References .
Einstein Bots	For each bot, regenerate the deployment code and update it on each web page that uses the bot. As part of the process, review and update the Permitted Domains field in the chat deployment settings. For more information, see Create Chat Deployments .
External software that accesses your Salesforce org	Update the references to your Salesforce URLs within the external software, then log in to Salesforce again via the software.
Hard-coded references to URLs	Update these references to your current My Domain URLs. Ideally, generate the hostnames via a dynamic method, such as the DomainCreator Class in Apex. If you deployed enhanced domains, review the hostnames redirections that stop in Winter '25. If you find any of those hostname formats in your org, update them to the enhanced domain format . For more information about updating hard-coded references, see Update References to Hard-Coded URLs for Lightning Experience in Salesforce Help and the knowledge article Updating Hard-Coded References .
Installed packages from AppExchange	Verify the package functionality. In necessary, log in to Salesforce again to access the package features. Note the features that require users to reconnect, and include those features in your end-user notifications. For more information, see Notify Users and Customers About a My Domain Change .
Firewalls and proxy servers that filter by hostname	Optionally, you can remove the hostnames that no longer apply to your org from your trust settings. However, we recommend that you allow those hostnames for redirection until all users and integrations are using your new domains successfully.
Pinned certificates	We don't recommend certificate pinning. Consider updating your policies to exclude pinned certificates. Otherwise, if you changed your My Domain suffix or deployed enhanced domains, review your pinned certificates against your new My Domain URLs, and update them as needed. If your software or policies require pinning, we recommend that you pin the intermediate certificate and not the leaf certificate.

Complete these tasks if your My Domain login URL changed. Your My Domain login URL changes when you change your My Domain name or suffix, deploy enhanced domains in a sandbox, or deploy partitioned domains in a non-production org.

Important: When your My Domain login URL or site URL changes, authentication methods such as SSO and MFA can stop working. Before you deploy a change to your My Domain, [preserve login access](#) for your admins and users.

Feature or Configuration	Action
API integrations into your org	<p>Check whether the API client references the server endpoint. For the API client, use the <code>metadataServerUrl</code> or <code>serverURL</code> value returned by a login request. Don't use a hard-coded server URL.</p> <p>After you deploy a My Domain change that affects your login URL, Salesforce returns the server URL containing your new My Domain name or suffix. If your org has been moved to another instance or you require SOAP API logins to use your My Domain in My Domain policies, old calls to instanced URLs fail. Otherwise, old calls to instance URLs continue to work. In either case, to avoid disruption, use the value returned by Salesforce.</p>
Branding	If your brand changed, update your login page branding. For more information, see Customize Your My Domain Login Page with Your Brand .
Desktop links	Update the desktop links with your new My Domain login URL.
DevOps Center	Update the named credentials used to authenticate users that access your org through DevOps Center. For more information, see Update Named Credentials After a My Domain Change .
Email templates	Replace references to the old URL with your new My Domain login URL. If the template uses a hard-coded URL, which is more common in email templates created in Salesforce Classic, we recommend that you update the template to use a dynamically generated URL.
Enablement sites (myTrailhead)	If your enablement site's login URL is your My Domain login URL in the format <code>https://MyDomainName.my.salesforce.com</code> , contact Salesforce Customer Support to update your authentication provider. For more information, see Configure Your Enablement Site .
Identity providers on your login page	Update your identity providers with your new My Domain login URL or new site login URL. For more information, see Update Authentication After a My Domain Change .
Knowledge articles served on your <code>*.my.salesforce.com</code> URL	Update any hard-coded references to the knowledge article URLs.
Messaging for In-App and Web	To update your Messaging for Web configuration with your My Domain login URL, republish your Messaging for Web deployment. For more information, see Update Your Messaging for Web Deployment After Upgrading to Enhanced Domains .
Lightning Out (beta)	<p>Update connected apps that use your My Domain login URL.</p> <p>Refresh the Lightning Out markup on Visualforce pages, web pages, and other locations that call your Lightning Out app.</p> <p>If authenticated users access Lightning Out, generate a new Session ID or authentication token for those connections.</p>

Feature or Configuration	Action
Multi-factor authentication for accessing Salesforce	Update your authentication configuration. For more information, see Update Authentication After a My Domain Change .
Named credentials	<p>Review the URL field for your named credentials. If a named credential uses your My Domain login URL, update the URL field with your new My Domain login URL. For more information, see Update Named Credentials After a My Domain Change.</p> <p>If users access functionality that relies on an updated named credential, instruct them to reauthenticate.</p>
Marketing Cloud Account Engagement (Pardot)	<p>If your Account Engagement configuration uses the Pardot Connector User, update the login URL that Account Engagement uses. In Account Engagement, update the Pardot Connector User. To use the same user, save the user again in Account Engagement. Then log out and back in to your org to complete the process.</p> <p>If you're using the Account Engagement Integration User, no changes are needed.</p> <p>When you deploy enhanced domains, no change to the Account Engagement tracker domain configuration is required.</p>
Open Computer-Telephony Integrations (CTIs), such as Salesforce Call Center and Click to Dial	<ul style="list-style-type: none"> • Verify with your telephony provider that your new URLs are included in the telephony provider's allowlists. Optionally, work with the provider to remove your previous URLs from their allowlists. • Update any hard-coded references to your previous URLs. Whenever possible, update these references to relative URLs instead. For examples, see the knowledge article Enhanced Domains and Open CTI with Visualforce (Spring '23).
A personalized version of the Salesforce mobile app published on the Google Play or Apple App stores	If your personalized version of the Salesforce app uses your My Domain login URL, update your app to use your new My Domain login URL.
Service Cloud Voice	<p>When you enable Service Cloud Voice, Salesforce uses your My Domain URLs to configure single sign-on (SSO) to your telephony provider. The required action depends upon your configuration.</p> <ul style="list-style-type: none"> • If you use Service Cloud Voice with Amazon Connect or Service Cloud Voice with Partner Telephony from Amazon Connect, no action is required. Salesforce updates your configuration, including the Amazon Connect allowlist, when you deploy your new My Domain. Optionally, remove your old URL formats from the Amazon Connect allowlist. • If you use Service Cloud Voice with Partner Telephony, work with your telephony provider to update your configuration with your new URLs after you deploy the new My Domain. In particular, update hard-coded connect API URLs, allowlists, and references to the Next generation Omni-Channel engagement URL that ends in <code>*.my.salesforce-scr.com</code>. Optionally, work with your telephony provider to remove your previous URL formats from their allowlist.
Single sign-on for accessing Salesforce	Update your authentication configuration. For more information, see Update Authentication After a My Domain Change .

Feature or Configuration	Action
Streaming API	<p>To ensure continuity during instance refreshes and org migrations, we recommend using My Domain URLs with Streaming API. If you follow this recommendation, replace your previous My Domain login URL with your new login URL.</p> <p>If you don't follow this recommendation yet, use your My Domain login URL with Streaming API. For example, replace <code>https://login.salesforce.com</code> and <code>https://InstanceName.salesforce.com/</code> with <code>https://MyDomainName.my.salesforce.com/</code>.</p> <p>For more information on logging in to Salesforce with your My Domain URL, see Log In to Salesforce with Code.</p>
Third-party connected apps	Work with the third party to update the URLs in the app, including SSO and other authentication configuration settings. For more information, see Update Authentication After a My Domain Change .
Zones for Experience Cloud sites (Ideas, Answers, Chatter Answers)	Update the email notification URL. From Setup, in the Quick Find box, enter <code>zones</code> , and then select Zones under Answers, Ideas Zones or Chatter Answers Zones . Then, next to the zone that you want to change, click Edit . To update the Email Notification URL, clear the existing URL so that the field is blank. Save the page, and the system populates the field with the new My Domain URL.

If the URL for your Visualforce pages changed, complete these tasks. Your Visualforce URL changes when you deploy enhanced domains or change your My Domain name.

 **Note:** If your My Domain login URL changed, these steps are covered in the corresponding list of post-deployment tasks in this Help topic.

Feature or Configuration	Task
Open Computer-Telephony Integrations (CTIs), such as Salesforce Call Center and Click to Dial	<ul style="list-style-type: none"> Verify that your new Visualforce URL is included in the telephony provider's allowlists. Optionally, work with the provider to remove your previous Visualforce URL from their allowlists. Update any hard-coded references to your previous Visualforce URL. Whenever possible, update these references to relative URLs instead. For examples, see the knowledge article Enhanced Domains and Open CTI with Visualforce (Spring '23).
Salesforce Maps	If you show nearby maps in Salesforce records or on sites, update the corresponding Maps Nearby Map component. See Add Nearby Maps to Salesforce Record Pages and Add Nearby Maps to Sites .
Service Cloud Voice	<p>If you use Service Cloud Voice with Partner Telephony, work with your telephony provider to update your configuration, including allowlists, with your new Visualforce URL. Optionally, work with your telephony provider to remove your previous Visualforce URL from their allowlist.</p> <p>If you use Service Cloud Voice with Amazon Connect or Service Cloud Voice with Partner Telephony from Amazon Connect, no action is required. Salesforce updates your configuration when you deploy your new My Domain. Optionally, you can update your Amazon Connect allowlist to remove your old Visualforce URL format.</p>

Complete these tasks if your content URL changed. That URL changes when you change your My Domain name or suffix, deploy enhanced domains in any org, or deploy partitioned domains in a non-production org.

Feature or Configuration	Task
Email and other document templates that use files hosted in Salesforce	Update the embedded content or images. For example, an icon or image that is hosted in your org and used in email footer templates. Instruct users to update their local templates.
Enablement sites (myTrailhead)	URLs for badge art stored in your Salesforce org changed. Update your modules and trails with the new badge art URLs. For more information, see Configure Your Enablement Site .
Web content that uses files hosted in Salesforce	Update the content links. For example, an image used on your website or externally published PDFs.

Complete these tasks if your Experience Cloud sites or Salesforce Sites URL changed. Site URLs change when you deploy enhanced domains, change your My Domain name in an org with enhanced domains, or deploy partitioned domains in a non-production org.

 **Important:** When your My Domain login URL or site URL changes, authentication methods such as SSO and MFA can stop working. Before you deploy a change to your My Domain, [preserve login access](#) for your admins and users.

Feature or Configuration	Task
Authentication that uses your site URL	If you configured a Salesforce authentication provider so that your users can log in to your custom external web app using their Salesforce credentials, verify your configuration. If your setup uses your site URL, update the configuration. For more information, see Update Authentication After a My Domain Change .
Branding	If your brand changed, update the branding for your Experience Cloud site login page. For more information, see Brand Your Pages from the Administration Workspace .
Desktop links	Update the desktop links with your new site login URL.
Email templates	Replace references to your old site URLs with the new site login URLs. Hard-coded URLs are more common in email templates created in Salesforce Classic.
Embedded Service Deployment (Chat)	Regenerate the Embedded Service code snippet with your new site URL. Update the web pages that include chat with the new snippet. See Add Your Embedded Chat to a Website .
Enablement sites (myTrailhead)	If your enablement site's login URL is your site URL, contact Salesforce Customer Support to update your authentication provider. For more information, see Configure Your Enablement Site .
External integrations	Update external integrations that reference your sites.
External links to the site	Update external-facing links such as publicly available Experience Cloud sites and Salesforce Sites. For example, a site URL can be used on your website, social media pages, marketing materials, and templates such as email signatures and automated responses.
Hard-coded references to your site within your sites and custom pages	Update any hard-coded links to Experience Cloud sites and Salesforce Sites in your sites and custom pages. For example, if you host knowledge articles on an Experience Cloud site, update the URLs that include your old site URL. These links are redirected to the equivalent current site URL until Winter '25 or until you disable the redirections. However, it's best to avoid hard-coded links. Use

Feature or Configuration	Task
	relative paths and dynamically generated hostnames whenever you can. If your site URL changes again in the future, relative paths and dynamically generated hostnames continue to work.
Identity providers on your site login page	Update your identity providers with your new site URL. For more information, see Update Authentication After a My Domain Change .
Knowledge articles served on your Experience Cloud site URL	Update any hard-coded references to the knowledge article URLs.
Lightning Out (beta)	Update connected apps that use your Experience Cloud URL. If authenticated users access Lightning Out, generate a new Session ID or authentication token for those connections.
Messaging for Web	If you use Messaging for Web in an Experience Builder site, update your allowlisted URLs. For more information, see Update Your Messaging for Web Deployment After Upgrading to Enhanced Domains .
A Mobile Publisher for Experience Cloud app	Update your app to use your new Experience Cloud sites URL before the redirection for your old site URL stops in Winter '25. For more information, see Mobile Publisher for Experience Cloud . If you use a custom domain such as <code>https://www.example.com</code> to host your Experience Cloud site and use that custom domain for your Mobile Publisher app, this task doesn't apply. Also, this task doesn't apply to Mobile Publisher for Lightning apps.
Multi-factor authentication for accessing your site	Update your authentication configuration. For more information, see Update Authentication After a My Domain Change .
Named credentials	Update named credentials that use your site login URL. For more information, see Update Named Credentials After a My Domain Change .
Single sign-on for accessing your site	If you configured SSO for your Experience Cloud sites, update the configuration. SSO options for sites include users logging in to your site with their Salesforce credentials or with an external provider's credentials. For more information, see Update Authentication After a My Domain Change .

If you have Experience Cloud sites and the My Domain change included enabling enhanced domains, complete this task.

Feature or Configuration	Task
Network restrictions that use IP allowlists only	When you deploy enhanced domains, your new system-managed Experience Cloud site <code>*.my.site.com</code> domain includes the Experience Cloud Content Delivery Network (CDN), which uses the Salesforce CDN Partner. The IP addresses used by the Salesforce CDN partner, Akamai, aren't published. Therefore, if your network settings include IP allowlisting, users can lose access to your site that uses the Salesforce CDN. For example, if your users log in via a VPN that exclusively uses IP allowlisting, the users on that VPN can't access your site, because it uses an Akamai IP address. To ensure that your users can access your Experience Cloud site on the Salesforce CDN, allowlist your site's domain, or serve your site via a custom domain. For more information, see the knowledge article Access Experience Sites via an IP-Restricted VPN After Enhanced Domains Deployment .

Feature or Configuration	Task
--------------------------	------

	If you can't allowlist your domain at the network level or configure a custom domain to serve your site, contact Salesforce Customer Support to disable the Salesforce CDN for your <code>*.my.site.com</code> site URL.
--	--

Complete these steps if the Experience Cloud sites or Salesforce Sites URL that Salesforce hosts changed and a custom domain such as `https://www.example.com` serves the site. Site URLs that Salesforce hosts change when you deploy enhanced domains, change your My Domain name in an org with enhanced domains, or deploy partitioned domains in a non-production org.

 **Note:** Enabling or disabling enhanced domains doesn't change the Salesforce internal `*.live.salesforce.com` CNAME for your custom domain.

Feature or Configuration	Task
--------------------------	------

Your custom domain uses the External HTTPS option: Use a third-party service or CDN to serve this domain.	Update the target hostname used when forwarding requests from your domain's proxy or CDN. For more information, see Prerequisites for a Custom Domain That Uses a Third-Party Service or CDN .
---	--

The custom domain serves the site via a non-Salesforce host or service.	Review and update the domain configuration, such as CDN settings and hard-coded references to Salesforce URLs.
---	--

SEE ALSO:

- [My Domain](#)
- [My Domain URL Formats](#)
- [My Domain Considerations](#)

Test My Domain Changes

Follow these guidelines to test My Domain changes and to ensure a smooth transition to the new My Domain URLs.

Test in a Sandbox

My Domain changes affect Salesforce login URLs, application URLs, and external-facing URLs such as Experience Cloud sites, Visualforce pages, and content files. To avoid end-user disruption, before you update production, it's important that you test My Domain changes in a sandbox.

When you test in a sandbox, note the changes required to complete successful tests. Use that list to update your org when you make the same My Domain changes in production.

 **Note:** When you enable and deploy enhanced domains in a sandbox, your My Domain login URL and the URLs for your Lightning pages and Lightning container components change. These URLs don't change when you enable and deploy enhanced domains in production unless you also change your My Domain name or suffix.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

Need a refresher on sandboxes? See [Sandboxes: Staging Environments for Customizing and Testing](#).

Update Your Org and Network Settings

When you change your My Domain details, your org's login URL and application URLs can change. URLs that are dynamically constructed by Salesforce use the new URLs automatically, but some Salesforce functionality requires more steps. Similarly, Apex code, JavaScript code, your network configuration, and existing data that contain the old URLs aren't automatically updated.

Ensure a smooth transition by updating references to your old URLs. For example, update your allowlists, custom Visualforce pages, the endpoint for API integration, and your identity providers with your new My Domain URLs. For more information, see [Update Your Org for My Domain Changes](#).

Disable Redirections During Testing

When you rename your My Domain, Salesforce redirects your previous My Domain URLs to your current My Domain. To identify any issues with access to your new My Domain URLs, we recommend that you disable all redirection options during your testing.

To help your users transition to your new My Domain URLs, you can enable these redirections again after you complete your testing.

For more information, see [My Domain Redirections](#).

Configure My Domain Policy Changes

The My Domain login policy determines whether users and SOAP APIs can use instanced URLs such as `https://na139.salesforce.com` to access your org in addition to the My Domain login URL.

 **Note:** This policy applies to all deployed and provisioned domains in the org.

For more information, see [Set the My Domain Login Policy](#).

Configure My Domain Settings

My Domain settings determine the user experience when logging into your Salesforce org via your My Domain. For example, you can customize your My Domain login page and add authentication services such as single sign-on (SSO). You can update these settings after you roll your domain changes, but it's better to set up and test them with your other My Domain changes. For more information, see [Configure My Domain Settings](#).

Prepare for Testing

Your Salesforce org's login and application URLs are used throughout Salesforce. For example, these URLs are used for API integrations, Experience Cloud sites, custom Visualforce pages, and custom apps. For more information, see [My Domain URL Formats](#).

 **Tip:** The My Domain Setup page shows your org's current My Domain login URL and the login URL for any My Domain change in progress. For the formats of the other URLs in your org, such as Visualforce pages, Salesforce Sites, and Experience Cloud sites, see [My Domain URL Formats](#).

If you enabled enhanced domains, or if you renamed your My Domain in an org with enhanced domains enabled, the URLs for Experience Cloud sites and Salesforce Sites change. Include verification of these external-facing URLs from all access points in your test plans. For example, a site URL can be used on your website, social media pages, marketing materials, and templates such as email signatures and automated responses.

To supplement your test plans, consider including users and partners in your testing. End-user testing can help validate the most commonly used workflows. And partners can help identify and remediate access issues efficiently.

Conduct Functional, End-User, and Integration Testing

Run automated and manual tests to ensure that they pass with your updated My Domain.

Automated tests can identify issues with accessing your org. However, these tests can miss items like broken links or content on a Visualforce page. To test for these issues, log in to Salesforce, and click tabs and links. To test your external-facing links, such as Experience Cloud sites, validate access from all available points as each user type. Then work with partners to validate integrations.

In your functional, end-user, and integration tests, include these common uses for Salesforce URLs.

- The end-user login process, including multi-factor authentication.
- Your custom My Domain login page.
- Integration access to your org, such as API calls, Apex code, and external apps and systems that access your Salesforce data or provide data to your org. Also include calls made via connected apps, Lightning Out (beta), and Embedded Service Deployment (Chat).
- Computer-Telephony Integrations (CTIs), such as Salesforce Call Center, Service Cloud Voice, and Click to Dial
- External-facing sites, such as Experience Cloud sites, as authenticated and unauthenticated guest users.
- Custom domains, such as `https://www.example.com`, that serve your Experience Cloud sites and Salesforce Sites.
- External integrations that reference your custom domains.
- If you have IP restrictions in place and you enabled enhanced domains, test access to your Experience Cloud sites and any custom domains that serve them via IPv6.
- SSO for your Salesforce org and your Experience Cloud sites.
- SAML SSO between your orgs and Experience Cloud sites.
- If you allow users to authenticate using alternate identity provider options directly from your My Domain login page, verify that login process with each available provider. Similarly, test all browser-based authentication methods for mobile users, if available in your org.
- If you configured a Salesforce authentication provider, your users can log in to your custom external web app using their Salesforce credentials. Verify that login process with each external web app.
- If you customized your org, for example, with buttons or Visualforce pages, make sure that you test your changes thoroughly. Look for broken links due to hard-coded references. For example, look for instance-based URLs such as `https://na139.salesforce.com`.



Tip: To search your Salesforce code, download the metadata. Then use a command-line interface such as [Salesforce CLI](#).

- Content stored in Salesforce, such as images and files. Multiple places can reference this content, including Visualforce pages, Experience Cloud sites, Salesforce Sites, and enablement sites (myTrailhead).
- Links to your Salesforce org from your sites, such as links to content, reports, files, and other sites.

Test Installed Packages

If you installed packages from [AppExchange](#), include the package-delivered functionality and components in your testing. Focus on components with links. For example, a package-delivered Visualforce page can contain links to your sites, content, or other Visualforce pages.



Note: In most cases, you can't edit package-delivered components. If you find that you can edit a package-delivered component, don't edit the component directly. Otherwise, the next package update can overwrite your changes.

We recommend that package developers use generated hostnames and relative paths to build any links. If they follow that approach, updated links work after a My Domain change, such as enabling enhanced domains. If you find an issue with components or functionality delivered by a package from AppExchange, contact the package developer. Make them aware of the issue so that they can publish a new version of their package that remediates the issue.

Test Again in Production

Before making My Domain changes in production, we highly recommend that you test those changes in a sandbox. Ideally, your sandbox includes all the functionality of production, but there can be obvious and not so obvious differences with production. For example, not all integration with third-party applications is available in sandboxes. And some data types, workflows, or complex test scenarios can only be tested in production. As a result, after you deploy a My Domain change in production, we recommend that you perform another round of testing.

Next Steps

After you complete testing, help your users get started using your new My Domain by providing links to pages that they use frequently, such as your login page. Let your users know if you changed the login policy, and encourage them to update their bookmarks the first time that they're redirected.

If you enabled enhanced domains, update external-facing links such as publicly available Experience Cloud sites and Salesforce Sites. For example, a site URL can be used on your website, social media pages, marketing materials, and templates such as email signatures and automated responses. Create a plan to update each location, and announce the change to your users and customers.

SEE ALSO:

[My Domain](#)

[Knowledge Article: Updating Hard-Coded References](#)

[Update References to Hard-Coded URLs for Lightning Experience](#)

My Domain Redirections

When you deploy a change to your My Domain, Salesforce redirects multiple hostnames automatically. Learn about the types of redirections, how to log redirections for the hostnames that Salesforce hosts for your org, and how you can control these redirections.

[Understand Redirections for Previous My Domain Hostnames](#)

After you deploy a change to your My Domain, Salesforce redirects your previous My Domain hostnames. If your org was created before Summer '22 and enhanced domains were deployed in your org, some of those redirections are temporary. And if your org was created before Summer '20, hostnames that contain your Salesforce instance can be redirected. Learn more about these directions and how you can control them.

[Manage My Domain Redirections](#)

Control whether users who visit your instanced URL, your previous My Domain URLs, or your previous *.force.com site URLs are redirected to the current My Domain URL. To help your users adopt the new URLs after a My Domain change, you can optionally enable a brief message during My Domain and *.force.com site URL redirections.

[Prepare for the End of Redirections for Non-Enhanced Domains](#)

After enhanced domains are deployed, your previous non-enhanced hostnames are redirected. Those redirections stop in Winter '25, starting in August 2024 for sandboxes. Review the affected hostnames and how you can disable the redirections to test before Salesforce disables them.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

[Disable or Remove Your Previous My Domain](#)

Each time that you deploy a change to your My Domain, Salesforce redirects requests from your previous My Domain URLs to your current My Domain. If you don't want these requests to be redirected, you can disable redirections from your previous My Domain. We recommend that you use this option when you test a My Domain change. Or, to use your previous My Domain in a different Salesforce org, remove your previous My Domain.

[Disable Redirections for Your Previous Force.com Site URLs](#)

When enhanced domains are deployed, the URL formats change for your Experience Cloud sites and Salesforce Sites. To minimize potential disruption, the `*.force.com` site URLs that Salesforce hosted for your sites are redirected to your My Domain current site URLs. If you prefer, you can disable these redirections.

[Log My Domain Hostname Redirections](#)

To reduce disruption, Salesforce redirects multiple hostnames automatically when you deploy a change to your My Domain. To better understand which previous My Domain hostnames are being redirected, enable event logging for these redirections.

SEE ALSO:

[My Domain](#)[Change Your My Domain Details](#)

Understand Redirections for Previous My Domain Hostnames

After you deploy a change to your My Domain, Salesforce redirects your previous My Domain hostnames. If your org was created before Summer '22 and enhanced domains were deployed in your org, some of those redirections are temporary. And if your org was created before Summer '20, hostnames that contain your Salesforce instance can be redirected. Learn more about these directions and how you can control them.

 **Note:** My Domain URL redirections help prevent disruption, but they're not intended as a permanent solution. Not all services work well with redirections, and a redirection adds a step to the process of loading the final web page. Also, Salesforce stops redirections of non-enhanced domains in Winter '25, starting in August 2024 for sandboxes. When you deploy a new My Domain, we highly recommend that you disable redirections during testing and update all references to your old URLs.

To see if redirections are in place for a previous My Domain, check the Redirections section of the My Domain Setup page.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Redirection Rules

Redirections for your org's previous hostnames follow different rules.

- For previous My Domain hostnames, Salesforce redirects your previous My Domain hostnames until you deploy another My Domain change or until you disable or remove your previous My Domain. All redirections from previous My Domain hostnames use redirect code 301 or redirect code 307.
- After you enhanced domains are deployed, your previous `*.force.com` site hostnames are redirected. Those redirections remain in place until you disable them or until Salesforce disables those redirections in Winter '25, starting in August 2024 for sandboxes.
- After you enable and deploy enhanced domains, other previous non-enhanced hostnames are redirected. These redirections remain in place until you disable them or until Salesforce disables those redirections in Winter '25. Also, if you deploy another change to your My Domain, these redirections stop.

- If your org was created before Winter '20, old bookmarks and links to your org can contain your Salesforce instance. For more information on these categories of hostnames and the purpose of each hostname, see [My Domain Hostnames](#). For information about restricting the hostnames that your users can use to access your org, see [Set the My Domain Login Policy](#) in Salesforce Help.

For all redirections, parameters passed via a URL follow these rules.

- The redirection includes query-string parameters up to the first hash (#), if present.
- The redirection doesn't include any hash fragments. A hash fragment is the part of the URL that includes a hash (#) and the text that follows it.
- For entity-containing requests, such as POST, the redirect includes a Temporary Redirect (307) HTTP response status code. That status code instructs the browser to retry the request at the new location via the original request method.

Limitations on My Domain Redirections

A redirection is an instruction sent to the requester of a URL, such as a browser, service, or search engine. During a call to one of your previous My Domain URLs, the Salesforce server responds with an HTTP status code and the new URL. The status code instructs the requester to use the new URL. The response also indicates that the previous My Domain URL is no longer valid so that the requester knows to update existing references to the previous URL.

When a user clicks a link to a previous My Domain URL, the browser is the requester, so the instructions are invisible to the user. In many cases, the user is unaware of the redirection unless you [enable a message](#) that notifies the user about the new URL.

However, there are some limitations on My Domain redirections. Here are the most common reasons why a call to a newly deployed My Domain URL isn't redirected, even though Salesforce sent the redirection instruction.

- Lack of support for redirections—The requester can't process the redirect instruction. In this case, to use the new URL, update the reference to the previous URL. Or you can work with the requester to get them to process the redirect request. Because of this limitation, My Domain redirections aren't intended as a permanent solution.
- Lack of access to the URL—If the user or service can't access the URL, the redirection fails. For example, if you restrict traffic on your network to specific domains and the new domain isn't on the allowlist, the user can't access the new URL. Also, IP restrictions can prevent users from accessing Salesforce features. Often the message that the user sees in these cases can help you determine the issue.
- A second My Domain deployment—When you deploy another My Domain change, existing redirections for your previous My Domain URLs stop. For more details on this situation, see the section in this topic on Previous My Domain Hostnames. This situation is another reason that My Domain redirections aren't intended as a permanent solution.

Previous My Domain Hostnames

Each time that you deploy a change to your My Domain details, Salesforce redirects your previous My Domain hostnames to the hostnames for your current My Domain. For example, your My Domain login URL is `example1.my.salesforce.com`, and you change it to `example2.my.salesforce.com`. Requests to `example1.my.salesforce.com` are redirected to `example2.my.salesforce.com`, and requests to `example1.lightning.force.com` are redirected to `example2.lightning.force.com`. Also, other customers can't use `example1` as a My Domain name.

 **Warning:** Before you deploy a My Domain change, consider the impact on any existing My Domain redirections. Salesforce only redirects your last set of previous My Domain URLs. If you previously changed your My Domain, your previous My Domain hostnames redirect to your current My Domain URLs unless you disable those redirections. When you deploy another My Domain change, existing redirections stop, and Salesforce redirects the My Domains in place before the latest deployment instead.

Let's look at some examples of how redirections are handled when you deploy a change to your My Domain and redirections are in place for previous My Domain hostnames.

In our first example, your old My Domain name is `example1`, and your current My Domain name is `example2`. You change your My Domain name a second time to `example3`. After you deploy this change, requests to `example2.my.salesforce.com` domain are redirected to `example3.my.salesforce.com`. Requests to `example1.my.salesforce.com` are no longer redirected, and other customers can use `example1` as their My Domain name.

This rule applies to any My Domain change that requires My Domain provisioning and deployment, such as enabling enhanced domains or enabling partitioned domains.

In our second example, after you change your My Domain name to `example3` and deploy the change, you enable enhanced domains. After you deploy the My Domain with enhanced domains, the non-enhanced hostnames for My Domain `example3` are redirected. For example, requests to `example3--c.visualforce.com` are redirected to `example3--c.vf.force.com`. However, requests to `example2.my.salesforce.com` are no longer redirected, and other customers can use `example2` as their My Domain name.

To stop redirections of your old My Domain hostnames, disable redirections for your previous My Domain. If your previous and current My Domain names are different, you can make that My Domain name available for use in other orgs by removing your previous My Domain. For more information, see [Disable or Remove Your Previous My Domain](#).

Hostnames That Change with Enhanced Domains

Enhanced domains meet the latest browser requirements and are enforced in all Salesforce orgs in Winter '24. With enhanced domains, all URLs across your org contain your company-specific My Domain name, including Experience Cloud sites and Salesforce Sites. The domain suffix also changes for multiple hostnames.

Here are a few examples of formats that change in a production org.

TYPE	FORMAT	ENHANCED DOMAIN URL FORMAT
Experience Cloud sites	Old	<i>ExperienceCloudSitesSubdomainName</i> .force.com
	New	<i>MyDomainName</i> .my.site.com
Lightning Container Component	Old	<i>MyDomainName--PackageName</i> .container.lightning.com
	New	<i>MyDomainName--PackageName</i> .container.force.com
Visualforce pages	Old	<i>MyDomainName--PackageName</i> .visualforce.com or <i>MyDomainName--PackageName.InstanceName</i> .visual.force.com or <i>MyDomainName--PackageName.InstanceName</i> .visual.sfdc- <i>HyperforceInstanceName</i> .force.com
	New	<i>MyDomainName--PackageName</i> .vf.force.com

For a full list of the hostnames that change, see [My Domain URL Format Changes When You Enable Enhanced Domains](#) in Salesforce Help. To better understand the purpose of each hostname type and whether it applies to you, see [My Domain Hostnames](#) in Salesforce Help.

Instanced Hostnames

Salesforce orgs created before Winter '20 didn't have a My Domain name by default. In this case, some users accessed Salesforce via hostnames that contain your Salesforce instance, such as `na87.lightning.force.com` in the URL.

`https://na87.lightning.force.com/lightning/page/home`. We don't recommend using hostnames that contain an instance name, because your Salesforce instance can change with an org migration or refresh.

A My Domain redirection setting determines what users see when they access a bookmark or link that contains your Salesforce instance. For example, when a user visits `https://InstanceName.lightning.force.com/lightning/page/home`, the Instance URL setting determines whether they're redirected to

`https://MyDomainName.lightning.force.com/lightning/page/home`. It also controls redirections for other instance URLs without your My Domain or site URL, such as Visualforce pages in the format

`https://PackageName.InstanceName.visual.force.com`. You can choose to redirect the user to the same page within the domain, with or without a warning, or to prevent redirections. For more information, see [Manage My Domain Redirections](#).

Temporary My Domain Redirections

To minimize potential disruption after you enable and deploy enhanced domains, Salesforce redirects your prior non-enhanced hostnames to the new hostnames, along with all of your other previous My Domain hostnames, by default. However, Salesforce stops the redirections for the non-enhanced hostnames in Winter '25, starting in August 2024 for sandboxes.

To test the impact when these redirections stop, temporarily disable the redirections from your previous My Domain. For more information, see [Prepare for the End of Redirections for Non-Enhanced Domains](#) and [Manage My Domain Redirections](#).

Track the Source of Redirections

When you rename your My Domain or deploy enhanced domains, external-facing URLs change. You can search the metadata for your org to determine where that URL is used in Salesforce, but discovering all the other places that your URL is used can be more complex. For example, a site URL can be used on your website, social media pages, marketing materials, and templates such as email signatures and automated responses. To help you identify these locations outside of Salesforce, the Hostname Redirects log includes the referrer and origin sent with each request that Salesforce redirects. For more information, see [Log My Domain Hostname Redirections](#).

SEE ALSO:

[My Domain](#)

[Enhanced Domains](#)

[My Domain Redirections](#)

Manage My Domain Redirections

Control whether users who visit your instanced URL, your previous My Domain URLs, or your previous *.force.com site URLs are redirected to the current My Domain URL. To help your users adopt the new URLs after a My Domain change, you can optionally enable a brief message during My Domain and *.force.com site URL redirections.

1. From Setup, in the Quick Find box, enter *My Domain*, and then select **My Domain**.
2. In the Redirections section, click **Edit**.
3. To redirect users who visit your previous My Domain URLs, select **Redirect previous My Domain URLs to your current My Domain**. This option is enabled by default after you deploy a My Domain change.
 - a. To notify users about the updated URL when they visit a previous My Domain URL, select **Notify users before redirecting to the current My Domain URL**. This setting applies only if redirections for your previous My Domain URLs are enabled.

If a previous My Domain URL (1) isn't listed, the settings that control redirections from previous My Domain URLs (2) are unavailable.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

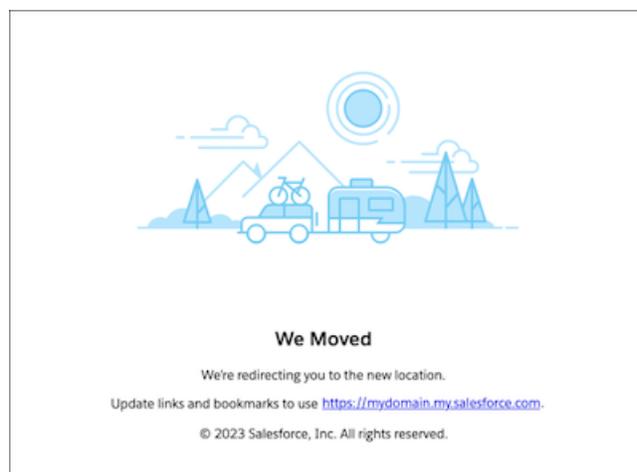
Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To edit My Domain settings:

- Customize Application

Here's an example of the message that users see when they visit a previous My Domain URL and both options are enabled.



4. If a *.force.com URL previously served your Experience Cloud sites or Salesforce sites, to redirect those URLs, select the option to redirect your old *.force.com site URLs. This option is enabled by default after enhanced domains are deployed.
 - a. To notify users know about redirections when they visit a previous *.force.com site URL, select **Notify users before redirecting to the current site URL**. This setting is available only when redirections for previous *.force.com site URLs are enabled.

Here's an example of the options to redirect your old *.force.com site URLs. This setting is enabled by default and lists the specific site URLs to be redirected. To see an example with your site URLs, hover over the information icon.

 **Warning:** These *.force.com redirections stop in Winter '25, even if this setting is enabled. For more information, see [Prepare for the End of Redirections for Non-Enhanced Domains](#).

5. Choose how to handle visits to your instanced URL.
 - a. To redirect users when they access URLs that don't include your My Domain name, select **Redirect to the same page within the domain**.

 **Note:** Bookmarks don't work when **Redirect to the same page within the domain** is selected for partner portals. Change the existing bookmarks manually to point to the new My Domain URL by replacing the Salesforce instanced URL with your My Domain URL. For example, replace `https://InstanceName.salesforce.com/` with `https://MyDomainName.my.salesforce.com/` in the bookmark's URL.
 - b. To remind users to use your My Domain URLs, select **Redirect with a warning to the same page within the domain**. Users briefly see a warning message, then they're redirected to the page. You can't customize the warning message. Select this option for a few days or weeks to help users transition to your new My Domain. The warning gives users a chance to change their bookmarks and get used to using the new URLs.
 - c. To require users to use your My Domain URLs when they view your pages, select **Don't redirect (recommended)**.

The Instanced URL redirection setting applies to your org's deployed and provisioned domains.

This setting determines what users see when they access a bookmark or link that contains your Salesforce instance. For example, when a user visits `https://InstanceName.lightning.force.com/lightning/page/home`, this setting determines whether they're redirected to `https://MyDomainName.lightning.force.com/lightning/page/home`.

6. Save your changes.

SEE ALSO:

[My Domain Redirections](#)

[Disable or Remove Your Previous My Domain](#)

[Disable Redirections for Your Previous Force.com Site URLs](#)

Prepare for the End of Redirections for Non-Enhanced Domains

After enhanced domains are deployed, your previous non-enhanced hostnames are redirected. Those redirections stop in Winter '25, starting in August 2024 for sandboxes. Review the affected hostnames and how you can disable the redirections to test before Salesforce disables them.

After enhanced domains are deployed, Salesforce redirects two categories of non-enhanced hostnames.

- Your previous *.force.com site hostnames are redirected until you disable these redirections or until Salesforce disables these redirections in Winter '25.
- Other previous non-enhanced hostnames are redirected until you disable those directions or until Salesforce disables those redirections in Winter '25. Also, if you deploy another change to your My Domain, these redirections stop.

To see if redirections are in place for a previous My Domain, check the Redirections section of the My Domain Setup page.

 **Note:** My Domain URL redirections help prevent disruption, but they're not intended as a permanent solution. Not all services work well with redirections, and a redirection adds a step to the process of loading the final web page. When you deploy enhanced domains, we highly recommend that you disable redirections during testing and update all references to your old URLs.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Track the Source of Redirections

You can search the metadata for your org to determine where the impacted URLs are used in Salesforce, but discovering all the other places that your URLs are used can be more complex. For example, site URLs and content URLs can be used on your website, social media pages, marketing materials, and templates such as email signatures and automated responses. To help you identify these locations outside of Salesforce, the Hostname Redirects log includes the referrer and origin sent with each request that Salesforce redirects. For more information, see [Log My Domain Hostname Redirections](#).

Notify Users During Redirections

To help your users update outdated links and bookmarks, display a brief message during the redirection that provides the current URL. See [Manage My Domain Redirections](#).

Previous *.force.com Site Hostnames

When you enable and deploy enhanced domains, the hostname formats change for your Experience Cloud sites and Salesforce Sites. To minimize potential disruption, the *.force.com hostnames that Salesforce hosted for your sites are redirected to your current site hostnames. Those redirections remain in place until Winter '25 or until you disable these redirections.

To disable these redirections for testing purposes, use an option in the Redirections section of the My Domain page and test. For more information, see [Disable Redirections for Your Previous Force.com Site URLs](#). For the replacement format for each of these hostnames,

see [My Domain URL Format Changes When You Enable Enhanced Domains](#). To better understand the purpose of each hostname type and whether it applies to you, see [My Domain Hostnames](#).

Here are the *.force.com site hostnames for a production org that are temporarily redirected after you enable and deploy enhanced domains.

- **ExperienceCloudSiteSubdomain**.force.com
- **SitesSubdomainName**.force.com
- **SitesSubdomainName**.secure.force.com

Here are the .*force.com site hostnames for a sandbox that are temporarily redirected after you enable and deploy enhanced domains.

- **SandboxName-ExperienceCloudSiteSubdomain.InstanceName**.force.com
- **SandboxName-SitesSubdomainName.InstanceName**.force.com

Other Non-Enhanced My Domain Hostnames

When you enable and deploy enhanced domains, your other previous non-enhanced My Domain hostnames are redirected. Those redirections remain in place until Winter '25 or until you disable these redirections.

For the type and the replacement format for each of these hostnames, see [My Domain URL Format Changes When You Enable Enhanced Domains](#). To better understand the purpose of each hostname type and whether it applies to you, see [My Domain Hostnames](#).

 **Note:** If you deploy another My Domain change after you enable and deploy enhanced domains, these hostnames are no longer redirected. For more information, see [Understand Redirections for Previous My Domain Hostnames](#).

To disable the redirections of these non-enhanced My Domain hostnames for testing purposes, you can temporarily disable your previous My Domain. For more information, see [Disable or Remove Your Previous My Domain](#).

Here are the non-enhanced hostnames for a production org that are temporarily redirected after you enable and deploy enhanced domains.

- **MyDomainName--PackageName**.container.lightning.com¹
- **MyDomainName--c**.documentforce.com
- **MyDomainName**.builder.salesforce-communities.com
- **MyDomainName**.livepreview.salesforce-communities.com
- **MyDomainName**.preview.salesforce-communities.com
- **MyDomainName--UniqueID**.a.forceusercontent.com
- **MyDomainName--UniqueID**.c.my.force-user-content.com
- **MyDomainName--PackageName**.visualforce.com¹
- **MyDomainName--c.InstanceName**.content.force.com
- **MyDomainName--sitestudio.InstanceName**.force.com
- **MyDomainName--livepreview.InstanceName**.force.com
- **MyDomainName--sitepreview.InstanceName**.force.com
- **MyDomainName--PackageName.InstanceName**.visual.force.com¹
- **MyDomainName--sitestudio.InstanceName.sfdc-HyperforceInstanceName**.force.com
- **MyDomainName--livepreview.InstanceName.sfdc-HyperforceInstanceName**.force.com
- **MyDomainName--sitepreview.InstanceName.sfdc-HyperforceInstanceName**.force.com
- **MyDomainName--c.InstanceName**.content.sfdc-HyperforceInstanceName.force.com

- *MyDomainName--PackageName.InstanceName.visual.sfdc-HyperforceInstanceName.force.com*¹

Here are the non-enhanced hostnames for a sandbox that are temporarily redirected after you enable and deploy enhanced domains.

- *MyDomainName--SandboxName.my.salesforce.com*
- *MyDomainName--SandboxName.lightning.force.com*
- *MyDomainName--SandboxName--PackageName.container.lightning.com*¹
- *MyDomainName--SandboxName--UniqueID.b.forceusercontent.com*
- *MyDomainName--SandboxName--UniqueID.c.forceusercontent.com*
- *MyDomainName--SandboxName--c.documentforce.com*
- *MyDomainName--SandboxName.builder.salesforce-communities.com*
- *MyDomainName--SandboxName.livepreview.salesforce-communities.com*
- *MyDomainName--SandboxName.preview.salesforce-communities.com*
- *MyDomainName--SandboxName.InstanceName.my.salesforce.com*
- *MyDomainName--SandboxName--PackageName.visualforce.com*¹
- *MyDomainName--SandboxName--c.InstanceName.content.force.com*
- *MyDomainName--SandboxName--sitestudio.InstanceName.force.com*
- *MyDomainName--SandboxName--livepreview.InstanceName.force.com*
- *MyDomainName--SandboxName--sitepreview.InstanceName.force.com*
- *MyDomainName--SandboxName--PackageName.InstanceName.visual.force.com*¹
- *MyDomainName--SandboxName--c.InstanceName.content.sfdc-HyperforceInstanceName.force.com*
- *MyDomainName--SandboxName--sitestudio.InstanceName.sfdc-HyperforceInstanceName.force.com*
- *MyDomainName--SandboxName--livepreview.InstanceName.sfdc-HyperforceInstanceName.force.com*
- *MyDomainName--SandboxName--sitepreview.InstanceName.sfdc-HyperforceInstanceName.force.com*
- *MyDomainName--SandboxName--PackageName.InstanceName.visual.sfdc-HyperforceInstanceName.force.com*¹

¹ If your installed package is unmanaged, the package name is c.

Instanced URLs Without My Domain

If your org was created before October 2020, you didn't get a My Domain by default. In that case, your users accessed Salesforce with these hostnames that contained your instance name but not your My Domain name. These hostnames are redirected if the Instanced URL setting in the Redirections section on the My Domain Setup page is set to **Redirect to the same page within the domain** or **Redirect with a warning to the same page within the domain**.

Redirections for these hostnames also stop in Winter '25. To disable the redirections of these hostnames for testing purposes, disable the redirections by updated the Instanced URL redirection setting to **Don't redirect (recommended)**. For more information, see [Set the My Domain Login Policy](#).

- *InstanceName.lightning.force.com*
- *ExperienceCloudSiteSubdomainName--builder.InstanceName.force.com*
- *ExperienceCloudSiteSubdomainName--preview.InstanceName.force.com*
- *ExperienceCloudSiteSubdomainName--live.InstanceName.force.com*
- *sitestudio.InstanceName.force.com*
- *sitepreview.InstanceName.force.com*
- *livepreview.InstanceName.force.com*

- `InstanceName--UniqueID.a.forceusercontent.com`
- `InstanceName--UniqueID.b.forceusercontent.com`
- `InstanceName--UniqueID.c.forceusercontent.com`
- `c.InstanceName.content.force.com`
- `PackageName.InstanceName.visual.force.com`¹
- `Region.scrpt.sfmc.sh`

¹ If your installed package is unmanaged, the package name is `c`.

SEE ALSO:

[My Domain Redirections](#)

[Enhanced Domains](#)

[Update Your Org for My Domain Changes](#)

[Test My Domain Changes](#)

Disable or Remove Your Previous My Domain

Each time that you deploy a change to your My Domain, Salesforce redirects requests from your previous My Domain URLs to your current My Domain. If you don't want these requests to be redirected, you can disable redirections from your previous My Domain. We recommend that you use this option when you test a My Domain change. Or, to use your previous My Domain in a different Salesforce org, remove your previous My Domain.

You can only access the options related to a previous My Domain after you deploy your new My Domain. If you change your My Domain more than one time, only the last My Domain for your org is redirected. For more information, see [My Domain Redirections](#) in Salesforce Help. To review the high-level steps and recommended practices for a My Domain change, including how to reduce the impact on your users and customers, see [Plan for a My Domain Change](#) in Salesforce Help.

 **Warning:** If you disable or remove your previous My Domain before a My Domain change is fully processed, calls to your org's custom domains, such as `https://www.example.com`, can return an error. To avoid this temporary disruption, wait 24 hours after changing your My Domain before removing your previous My Domain if your custom domain uses one of these HTTPS options:

- Serve the domain with the Salesforce Content Delivery Network (CDN)
- Use a temporary non-HTTPS domain

1. From Setup, in the Quick Find box, enter `My Domain`, and then select **My Domain**.

If URLs for a previous My Domain are being redirected to your current My Domain, the previous My Domain URL is listed under Redirections.

2. Under Redirections, click **Edit**.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To edit My Domain settings:

- Customize Application

To define a My Domain name:

- Customize Application
- AND
- Modify All Data

Redirections Save Cancel

Previous My Domain URL mycompany.my.salesforce.com without enhanced domains

Remove Previous My Domain ⓘ

My Domain URLs

- Redirect previous My Domain URLs to your current My Domain ⓘ
- Notify users before redirecting to the current My Domain URL
- Redirect portal-mycompany.force.com and mycompany.force.com URLs to your current My Domain site URLs ⓘ
- Notify users before redirecting to the current site URL
- Log redirections ⓘ

Instanced URL Specify the behavior when a user attempts to access this org via a URL that starts with https://eu55.salesforce.com. If a My Domain change is in progress, this setting also applies to the provisioned domains for this org.

- Redirect to the same page within the domain
- Redirect with a warning to the same page within the domain
- Don't redirect (recommended)

Save Cancel

- To disable redirections from your previous My Domain, deselect **Redirect previous My Domain URLs to your current My Domain** and save your changes. Or, to enable redirections from your previous My Domain, select this option.

This option determines what happens when users visit bookmarks or links that contain your previous My Domain name. For example, when a user visits `https://PreviousMyDomainName.lightning.force.com/lightning/page/home`, this option determines whether they're redirected to

`https://CurrentMyDomainName.lightning.force.com/lightning/page/home`.

When you disable this option, you enforce your My Domain change. Salesforce recommends that you temporarily disable redirections from your previous My Domain to test a My Domain change or to test the effect of removing your previous My Domain.

 **Note:** This setting only controls redirections from URLs associated with the My Domain in the Previous My Domain URL section. For information on controlling redirections from your instanced URL, such as `https://eu55.salesforce.com`, and from previous `*.force.com` site URLs, see [Manage My Domain Redirections](#).

- To permanently remove your previous My Domain, click **Remove Previous My Domain**, and confirm your decision.

 **Note:** To avoid user disruption, we recommend that you test before you remove your previous My Domain. To test the effect of disabling redirections, deselect **Redirect previous My Domain URLs to your current My Domain**, and save your changes. After you complete your testing, use the **Remove Previous My Domain** option to remove your previous My Domain.

After you remove your previous My Domain, requests to your previous My Domain's URLs are no longer redirected. If your previous and current My Domain names are different, your previous My Domain name is now available for use in other orgs.

To avoid potential conflicts between follow-up processes such as CNAME and DNS updates, you can't make a change that requires provisioning for 15 minutes after you remove your previous My Domain. Changes that require provisioning include changing your My Domain name or suffix, enabling enhanced domains, and moving to Salesforce Edge Network.

SEE ALSO:

[My Domain Redirections](#)
[My Domain Considerations](#)
[My Domain URL Formats](#)

Disable Redirections for Your Previous Force.com Site URLs

When enhanced domains are deployed, the URL formats change for your Experience Cloud sites and Salesforce Sites. To minimize potential disruption, the `*.force.com` site URLs that Salesforce hosted for your sites are redirected to your My Domain current site URLs. If you prefer, you can disable these redirections.

You can enable or disable redirections from previous `*.force.com` site URLs only if your enhanced domains are enabled and Salesforce previously hosted a `*.force.com` site URL for your org.

1. From Setup, in the Quick Find box, enter *My Domain*, and then select **My Domain**.
Any URLs that end in `.force.com` that Salesforce previously served your Experience Cloud sites URL or Salesforce Sites are listed under Redirections.
2. Under Redirections, click **Edit**.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To edit My Domain settings:

- Customize Application

Redirections [Save] [Cancel]

Previous My Domain URL mycompany.my.salesforce.com with enhanced domains
[Remove Previous My Domain] ⓘ

My Domain URLs

- Redirect previous My Domain URLs to your current My Domain ⓘ
- Notify users before redirecting to the current My Domain URL ⓘ
- Redirect portal-mycompany.force.com and mycompany.force.com URLs to your current My Domain site URLs ⓘ
- Notify users before redirecting to the current site URL ⓘ
- Log redirections ⓘ

Instanced URL Specify the behavior when a user attempts to access this org via a URL that starts with `https://eu55.salesforce.com`. If a My Domain change is in progress, this setting also applies to the provisioned domains for this org.

- Redirect to the same page within the domain
- Redirect with a warning to the same page within the domain
- Don't redirect (recommended)

[Save] [Cancel]

The option to redirect your old `*.force.com` site URLs is enabled by default and lists the specific site URLs to be redirected. To see a specific example, hover over the information icon.

 **Warning:** These `*.force.com` redirections stop in Winter '25, even if this setting is enabled. For more information, see [Prepare for the End of Redirections for Non-Enhanced Domains](#).

3. To disable redirects for the displayed `*.force.com` URLs, deselect this option and save your changes.

When you disable this option, users that visit those `*.force.com` URLs see a File Not Found error. This error also displays when users visit any custom domains such as `https://www.example.com` that serve those `*.force.com` URLs.

To enable the redirections again, select the same option and save your changes. For more information, see [Manage My Domain Redirections](#).

SEE ALSO:

[My Domain Redirections](#)

[Configure My Domain Settings](#)

Log My Domain Hostname Redirections

To reduce disruption, Salesforce redirects multiple hostnames automatically when you deploy a change to your My Domain. To better understand which previous My Domain hostnames are being redirected, enable event logging for these redirections.

 **Note:** The Hostname Redirects event is free for all customers with a 24-hour data retention period. This event is available in the API but not in the Event Monitoring Analytics app. You can also download the Hostname Redirects event log file on the My Domain page.

1. From Setup, in the Quick Find box, enter *My Domain*, and then select **My Domain**.
2. In the Redirections section, click **Edit**.
3. Select **Log redirections** and save your changes.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To edit My Domain settings:

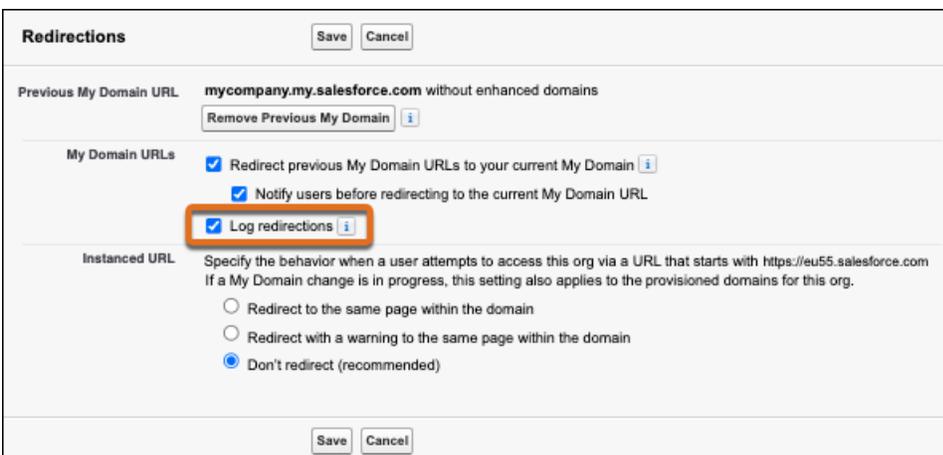
- Customize Application

To access and download event log files:

- View All Data

OR

View Event Log Files AND API Enabled



Redirections [Save] [Cancel]

Previous My Domain URL **mycompany.my.salesforce.com** without enhanced domains
 [Remove Previous My Domain] ⓘ

My Domain URLs

- Redirect previous My Domain URLs to your current My Domain ⓘ
- Notify users before redirecting to the current My Domain URL
- Log redirections** ⓘ

Instanced URL Specify the behavior when a user attempts to access this org via a URL that starts with `https://eu55.salesforce.com`. If a My Domain change is in progress, this setting also applies to the provisioned domains for this org.

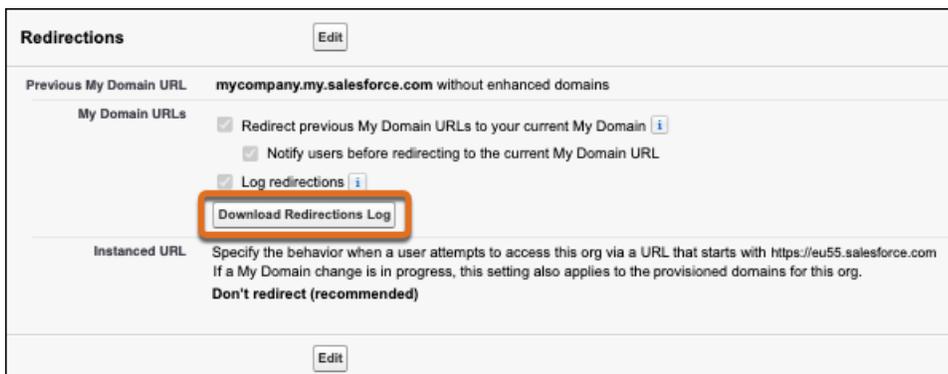
- Redirect to the same page within the domain
- Redirect with a warning to the same page within the domain
- Don't redirect (recommended)

[Save] [Cancel]

 **Note:** This option and the Redirections section are available only after you deploy a My Domain change.

After you save your changes, Salesforce produces a log for the Hostname Redirects event type in the next daily run. Salesforce uploads event log files after they're generated. Most dataset uploads finish around the same time each day. Exact finish times vary depending on dataset size and content.

You can also download the latest incremental daily Hostname Redirects log by clicking **Download Redirections Log** from the My Domain Setup page.



The screenshot shows the 'Redirections' configuration page. At the top, there is an 'Edit' button. Below it, the 'Previous My Domain URL' is 'mycompany.my.salesforce.com without enhanced domains'. Under 'My Domain URLs', there are three checked options: 'Redirect previous My Domain URLs to your current My Domain', 'Notify users before redirecting to the current My Domain URL', and 'Log redirections'. The 'Download Redirections Log' button is highlighted with a red box. Below this, the 'Instanced URL' is set to 'Don't redirect (recommended)'. At the bottom, there is another 'Edit' button.

The log file includes a summary of hostname redirection activity for the last 24 hours at the time that the background process generates the file. After you enable this feature, the next log file includes only the redirections that occurred after you enabled redirection logging. If your last My Domain change included enabling and deploying enhanced domains, the log includes redirections for the old hostnames listed on [My Domain URL Format Changes When You Enable Enhanced Domains](#). The log doesn't include redirections for generic instanced hostnames, such as `na87.salesforce.com`.

Only one hostname redirection log file is available at a time. When the daily incremental event log file is generated during the daily background process, the new file replaces the existing file. When you download the redirections log from the My Domain Setup page, you get the latest daily log file in CSV format.

If the log file doesn't exist, either the log generation process hasn't run yet or there's no redirection data to report for that 24-hour window. The log file is generated only when at least one redirection occurred for the day.

 **Note:** To keep the size of the log file manageable, the log includes one entry for each redirected hostname and path combination within an hour. As a result, the log includes all redirected hostnames and path combinations, but only includes the first redirection within each hour.

For example, if `https://MyCompany.my.site.com/shop` is redirected at 02:01 PM and `https://MyCompany.my.site.com/shop?q=sneakers` is redirected for another user at 02:02 PM, only the redirection that occurred at 02:01 PM is captured for `MyCompany.my.site.com/shop` for that hour. But if `https://MyCompany.my.site.com/help` is redirected at 2:05 PM, that redirection is captured on a new line because the `MyCompany.my.site.com/help` hostname and path combination differs from `MyCompany.my.site.com/shop`.

Similarly, if the redirection of `https://MyCompany.my.site.com/contactUs` is blocked at 07:02 AM and `https://MyCompany.my.site.com/contactUs` is redirected at 07:11 AM, only the blocked redirection for `MyCompany.my.site.com/contactUs` is captured in the log for that hour.

To help you identify the locations where your URL is used, the log includes the referrer and origin sent in the corresponding HTTP headers with each request that Salesforce redirects. The requester controls the values passed in these HTTP Headers, so fields can contain a null value. For details about this behavior and about other fields within the log file, see Hostname Redirects in the Object Reference for the Salesforce Platform.

To collect hostname redirection logs for multiple days, schedule a daily query of the Hostname Redirects event type via REST API. For example, you can configure a cron job in Unix or a scheduled task in Windows to run the query.

SEE ALSO:

[My Domain Redirections](#)

[Object Reference for the Salesforce Platform: Hostname Redirects Event Type](#)

[Trailhead: Event Monitoring](#)

[REST API Developer Guide: Using Event Monitoring](#)

Configure My Domain Settings

Determine the user experience when logging into your Salesforce org via your My Domain. Manage user logins and authentication methods and customize your login page with your brand. Control whether users are redirected when they visit URLs that Salesforce previously served for your org.

 **Note:** My Domain settings apply to your org's deployed and provisioned domains.

[Set the My Domain Login Policy](#)

Manage how users and API calls access your Salesforce org. Specify whether logins to your org require your My Domain. And choose what users see when they access a bookmark or link that contains your instance-specific domain.

[Customize Your My Domain Login Page with Your Brand](#)

My Domain gives you a point-and-click way to brand the page that prompts users to log in to your Salesforce org. You can replace the Salesforce logo with your own and change your background and login button colors. You can also display content to the right of your login form. Branding options apply to the entire login experience, including pages for users to verify their identity and reset passwords. They also apply to login flows.

[Create an Interview-Based Login Page with My Domain Login Discovery](#)

Configure My Domain with Login Discovery to simplify the login process for users. Login Discovery is sometimes called interview-based login because it's a two-step process. First, users identify themselves with an email address or phone number at the login page. Next, users verify themselves depending on the identifier entered. Users can verify themselves with a password, their single sign-on (SSO) credentials, or Lightning Login. You set up Login Discovery from the My Domain Setup page after you create an Apex class that implements the `MyDomainLoginDiscoveryHandler` interface.

[Add Identity Providers to the My Domain Login Page](#)

Users can authenticate with alternate identity provider options from your My Domain login page. If you enabled single sign-on (SSO) and configured SAML, or if you set up external authentication providers, you can display them on the login page. Users are sent to the identity provider's login screen to authenticate and then redirected to Salesforce.

[Customize Your My Domain Login Page for Mobile Auth Methods](#)

By default, mobile apps built with Salesforce Mobile SDK use standard authentication. With standard authentication, a user logs in and approves access to their Salesforce data within the mobile app. For improved security and better performance on mobile apps, configure advanced browser-based authentication from the My Domain Setup page. With browser based-authentication, mobile users are taken to their native browser for authentication. After they log in and approve data access, they're redirected to the mobile app.

SEE ALSO:

[My Domain](#)

EDITIONS

Available in: both Salesforce Classic (**not available in all orgs**) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Set the My Domain Login Policy

Manage how users and API calls access your Salesforce org. Specify whether logins to your org require your My Domain. And choose what users see when they access a bookmark or link that contains your instance-specific domain.

 **Note:** This setting applies to your org's deployed and provisioned domains.

To choose how to handle requests to your instanced URL, such as `https://eu55.salesforce.com`, and requests to your previous My Domain URLs, see [Manage My Domain Redirections](#).

1. From Setup, in the Quick Find box, enter *My Domain*, and then select **My Domain**.
2. In the Routing and Policies section, click **Edit**.
3. To require that users log in with your My Domain in production, select **Prevent login from `https://login.salesforce.com`**. Or, in a sandbox, select **Prevent login from `https://test.salesforce.com`**.

When you enable this setting, users also can't use your instanced URL, such as `https://na77.salesforce.com`, to log in. Also, when you enable **Prevent login from `https://test.salesforce.com`** in a sandbox, admins can't log in to that sandbox via the **Log In** action on the Sandboxes Setup page.

4. To require that SOAP API logins use your My Domain login URL, in production, select **Prevent SOAP API login from `https://login.salesforce.com`**. Or, in a sandbox, select **Prevent login from `https://test.salesforce.com`**.
When you enable this setting, SOAP API logins also can't use your instanced URL, such as `https://na77.salesforce.com`, to log in.
5. Save your changes.

SEE ALSO:

- [Configure My Domain Settings](#)
- [Manage My Domain Redirections](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To edit My Domain settings:

- Customize Application

Customize Your My Domain Login Page with Your Brand

My Domain gives you a point-and-click way to brand the page that prompts users to log in to your Salesforce org. You can replace the Salesforce logo with your own and change your background and login button colors. You can also display content to the right of your login form. Branding options apply to the entire login experience, including pages for users to verify their identity and reset passwords. They also apply to login flows.

 **Note:** Authentication configuration settings apply to your org's deployed and provisioned My Domains.

1. From Setup, in the Quick find box, enter *My Domain*, and then select **My Domain**.
2. Under Authentication Configuration, click **Edit**.
3. To customize your logo, click **Choose File**, and upload an image file.
Images can be .jpg, .gif, or .png files up to 100 KB. The maximum image size is 250 px by 125 px.
4. To customize your login page background, click , and choose your hexadecimal color code.
5. To display content in the right frame URL, enter a URL.
By default, the right side shows the current Salesforce promotions, <https://c.salesforce.com/login-messages/promos.html>, in an iframe. The iframe creates an inline frame, which embeds an HTML document into the current page.
You can show your own content by supplying a URL that uses SSL encryption and the https:// prefix. The iframe dynamically expands to fill about 50% of the page. If you don't have a URL handy, you can use <https://www.example.com/> to see how a right frame URL displays on your login page.
To build your own custom iframe with responsive web design, use the [My Domain Sample](#) template.
6. Save your changes.

SEE ALSO:

[Configure My Domain Settings](#)

[Add Identity Providers to the My Domain Login Page](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To customize a My Domain login page:

- [Customize Application](#)

Create an Interview-Based Login Page with My Domain Login Discovery

Configure My Domain with Login Discovery to simplify the login process for users. Login Discovery is sometimes called interview-based login because it's a two-step process. First, users identify themselves with an email address or phone number at the login page. Next, users verify themselves depending on the identifier entered. Users can verify themselves with a password, their single sign-on (SSO) credentials, or Lightning Login. You set up Login Discovery from the My Domain Setup page after you create an Apex class that implements the `MyDomainLoginDiscoveryHandler` interface.

Login Discovery eliminates the onerous task of managing forgotten usernames. With Login Discovery, your users can log in with something they're likely to remember, like their email address or phone number. Also, if your org is configured with multiple identity providers (IdP) for SSO, Login Discovery can direct users to the suitable IdP. If your login page contains an SSO button along with the username and password fields, users can miss the button or not know what it's used for. If you're using Login Discovery, no decisions are required.

Login Discovery is helpful when you have different login processes depending on the situation, such location or device type. For example, if you have separate IdPs for mobile and desktop users. Instead of having a login page with buttons for both, Login Discovery determines where users are logging in from and directs them to the suitable IdP.

To configure Login Discovery for My Domain, create a handler in Apex and then reference the handler from the My Domain Setup page. The Apex class implements the `MyDomainLoginDiscoveryHandler` interface. The handler includes logic that defines how to look up a user based on the identifier value entered on the login page. Then it determines which authentication service to invoke.

 **Note:** Authentication configuration settings apply to your org's deployed and provisioned My Domains.

1. From Setup, in the Quick Find box, enter *My Domain*, and then select **My Domain**.
2. Under Authentication Configuration, click **Edit**.
3. For Login Page Type, select **Discovery**.
4. Optionally, for Login Prompt, enter the text or custom label.
For example, you can use a custom label to localize the text, such as `$Login.loginPrompt`.
5. Locate the Login Discovery Handler that you created by implementing the `MyDomainLoginDiscoveryHandler` interface. From Setup, in the Quick Find box, enter *Apex Classes*, and then select **Apex Classes**. Select the handler from the list.
6. Optionally, for Execute Login As, choose a Salesforce admin with Manage Users permission.
By default, the handler runs in system mode.
7. Save your changes.

 **Tip:** If you can't log in after setting up Login Discovery, modify the URL to return to the standard login page, which prompts for a username and password. You can add `login` as a URL query string parameter, for example, `https://MyDomainName.my.salesforce.com/?login`. Or you can add `login=true` to the URL, for example, `https://MyDomainName.my.salesforce.com/?login=true`.

SEE ALSO:

- [Configure My Domain Settings](#)
- [Verify Email Addresses with Async Email](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

EDITIONS

User Permissions Needed

To customize a My Domain login page:	Customize Application
--------------------------------------	-----------------------

Add Identity Providers to the My Domain Login Page

Users can authenticate with alternate identity provider options from your My Domain login page. If you enabled single sign-on (SSO) and configured SAML, or if you set up external authentication providers, you can display them on the login page. Users are sent to the identity provider's login screen to authenticate and then redirected to Salesforce.

Available authentication services include all providers configured as SAML SSO identity providers or external authentication providers, except Janrain. You can't use Janrain for authentication from the login page.

 **Note:** Authentication configuration settings apply to your org's deployed and provisioned My Domains.

1. From Setup, in the Quick Find box, enter *My Domain*, and then select **My Domain**.
2. Under Authentication Configuration, click **Edit**.
3. Select the authentication services that you want to make available on the login page.
4. Save your changes.

You can list all your org's available SSO identity providers on your login page. If you have several, consider setting up your login page with the Login Discovery page type.

SEE ALSO:

[Configure My Domain Settings](#)

[Customize Your My Domain Login Page with Your Brand](#)

Customize Your My Domain Login Page for Mobile Auth Methods

By default, mobile apps built with Salesforce Mobile SDK use standard authentication. With standard authentication, a user logs in and approves access to their Salesforce data within the mobile app. For improved security and better performance on mobile apps, configure advanced browser-based authentication from the My Domain Setup page. With browser-based authentication, mobile users are taken to their native browser for authentication. After they log in and approve data access, they're redirected to the mobile app.

Browser-based authentication is required for mobile users logging in to your My Domain URLs with these authentication methods.

- Certificate-based login
- Single sign-on (SSO) configurations that use certificates

For SSO configurations that don't use certificates, browser-based authentication is recommended for better performance but not required. If you set up browser-based authentication with Google as an SSO identity provider, mobile users who are already logged in to Google aren't required to log in again. When your mobile app directs users to their native browser for authentication, they can select an option to continue with their Google account. With standard authentication, users don't get this benefit.

Browser-based authentication is also supported for delegated authentication and authentication with Windows NT LAN Manager (NTLM).

Changing these settings can break your mobile authentication flows. We recommend testing your changes in a sandbox before you implement them in production.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To customize a My Domain login page:

- Customize Application

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To customize a My Domain login page:

- Customize Application

 **Note:** Authentication configuration settings apply to your org's deployed and provisioned My Domains.

1. From Setup, in the Quick Find box, enter *My Domain*, and then select **My Domain**.
2. Under Authentication Configuration, click **Edit**.
3. Select **Use the native browser for user authentication on iOS** or **Use the native browser for user authentication on Android**.
With these settings selected, mobile users are directed to Safari if using iOS, and to Chrome if using Android.
4. Save your changes.

Advanced browser-based authentication also requires some configuration in your mobile app. For more information, see [Using Advanced Authentication](#) in the Mobile SDK Development Guide.

SEE ALSO:

[Configure My Domain Settings](#)

[Mobile SDK Development Guide: Configuring Advanced Authentication in iOS Apps](#)

[Mobile SDK Development Guide: Upgrading Android Single Sign-On Apps to Google Login Requirements](#)

Salesforce Edge Network

Users access your Salesforce data from all over the world. Salesforce Edge Network delivers a consistent user experience regardless of a user's location. It improves download times and the user's network experience. The move to Salesforce Edge Network is seamless for your users. They keep using the same URLs to access your org, only with a better experience.

Government Cloud is currently excluded from Salesforce Edge Network. Most custom domains, such as `https://www.example.com`, that serve your Salesforce Sites and Experience Cloud sites aren't supported on Salesforce Edge Network. For more information on Salesforce Edge Network restrictions for custom domains, see [Considerations for Salesforce Edge Network](#).

Salesforce Edge Network is available on a rolling basis starting in Summer '23. If you're not already on Salesforce Edge Network, prepare for the move by reviewing this [Enable Salesforce Edge Network for your Domain](#) knowledge article.

[What Is Salesforce Edge Network?](#)

Salesforce Edge Network is a network technology that improves download times for users around the globe. Users get a better network experience while remaining on the Salesforce trusted infrastructure, which protects, uses, and processes data appropriately and in accordance with the law.

[Considerations for Salesforce Edge Network](#)

Find out how to prepare your org to use Salesforce Edge Network. In particular, know which URLs can't be routed through Salesforce Edge Network.

[Route My Domain Through Salesforce Edge Network](#)

Improve download times and the user experience by routing your My Domain through Salesforce Edge Network. As business becomes more global, users access your Salesforce data from all over the world. Salesforce Edge Network delivers a consistent user experience regardless of a user's location.

SEE ALSO:

[My Domain](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

What Is Salesforce Edge Network?

Salesforce Edge Network is a network technology that improves download times for users around the globe. Users get a better network experience while remaining on the Salesforce trusted infrastructure, which protects, uses, and processes data appropriately and in accordance with the law.

Instead of sending network requests directly to the Salesforce data center, Salesforce Edge Network directs requests to the closest Salesforce location where Salesforce Edge Network is deployed. At that location, Salesforce Edge Network provides a range of services.

Providing these services closer to the customer reduces the round-trip time for certain requests. Customer requests are then sent to the Salesforce data center using Salesforce secure, optimized, high-bandwidth connections.

- **TLS termination**—Transport Layer Security (TLS) establishes secure connections to Salesforce. Salesforce Edge Network enables end-to-end secure connections with persistent TLS connections and optimized setup, reducing the connection setup time.
- **Caching of static content**—Caching is limited to the content with HTTP headers marked as cacheable by Salesforce or customer integrations. This content is typically publicly available content such as JavaScript and CSS files.
- **Intelligent routing of user requests to the closest data center**—Salesforce automatically sends users to the most optimal point of presence based on its network data.
- **TCP optimizations**—Transmission Control Protocol (TCP) optimizations help data move more quickly and efficiently across the network.

SEE ALSO:

[My Domain](#)

[Considerations for Salesforce Edge Network](#)

[Route My Domain Through Salesforce Edge Network](#)

Knowledge Article: Enable Salesforce Edge Network for your Domain

Considerations for Salesforce Edge Network

Find out how to prepare your org to use Salesforce Edge Network. In particular, know which URLs can't be routed through Salesforce Edge Network.

Prerequisites

Prepare your org before activating Salesforce Edge Network.

- If you allowlist Salesforce IP addresses by region, Salesforce recommends that you include our current IP address ranges for regions where you have end users.
- If you use client-side certificate pinning to validate the server's certificate, Salesforce doesn't recommend pinning leaf certificates. Because Salesforce Edge Network uses data center specific certificates, Salesforce recommends that you pin the intermediate certificate instead for a better experience.

 **Note:** Keep these things in mind if you're considering enabling Salesforce Edge Network.

- Government Cloud is currently excluded from Salesforce Edge Network.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

- Hyperforce customers using [apex:page](#) Visualforce page enable global caching with Salesforce Edge.
- Salesforce Edge Network can be disabled by Salesforce Customer Support.

URL Routing

To maximize the number of URLs that are routed through Salesforce Edge Network, enable enhanced domains after your org is on Salesforce Edge Network. With enhanced domains, all URLs across your org include your company-specific My Domain name, and instance names are removed from your org's URLs.

When you enable Salesforce Edge Network, most of your My Domain URLs are routed through it. However, note these exceptions.

- URLs that contain your Salesforce instance name. See which My Domain URLs contain your instance name in My Domain URL Formats.
- URLs associated with custom domains, such as `https://www.example.com`, that serve your org's Salesforce Sites or Experience Cloud sites and don't use the HTTPS option: Serve the domain with your HTTPS certificate on Salesforce servers.
- Salesforce Sites and Experience Cloud sites with domains ending in `.force.com`
- URLs associated with Customer 360 Data Manager that end with `.admin.salesforce-hub.com` and `.my.salesforce-hub.com`
- URLs associated with Live Agent Chat that end with `.my.salesforcescrt.com` or `.my.salesforce-scrt.com`
- URLs associated with untrusted content domains
- URLs associated with orgs in Government Isolated Architecture (GIA) data centers

We're in the process of migrating custom domains, such as `https://www.example.com`, that serve your Experience Cloud sites to Salesforce Edge Network. This change only applies to custom domains that use the HTTPS option: Serve the domain with your HTTPS certificate on Salesforce servers. To determine whether your qualifying custom domain uses Salesforce Edge Network, look for references to edge when you view your custom domain's HTTP headers, or resolve the domain name. For more information, see the Knowledge Article, [What is Salesforce Edge Network?](#)

SEE ALSO:

[My Domain Provisioning and Deployment](#)

[Route My Domain Through Salesforce Edge Network](#)

[My Domain URL Formats](#)

[Enhanced Domains](#)

Knowledge Article: [Salesforce IP Addresses and Domains to Allow](#)

Knowledge Article: [What is Salesforce Edge Network?](#)

Knowledge Article: [Enable Salesforce Edge Network for your Domain](#)

Route My Domain Through Salesforce Edge Network

Improve download times and the user experience by routing your My Domain through Salesforce Edge Network. As business becomes more global, users access your Salesforce data from all over the world. Salesforce Edge Network delivers a consistent user experience regardless of a user's location.

To route your My Domain through Salesforce Edge Network, you must have a deployed My Domain. Government Cloud is currently excluded from Salesforce Edge Network.

 **Note:** Salesforce Edge Network is available on a rolling basis starting in Summer '23. If you're not already on Salesforce Edge Network, prepare for the move by reviewing this [Enable Salesforce Edge Network for your Domain](#) knowledge article.

Prepare your org before activating Salesforce Edge Network. If you allowlist Salesforce IP addresses by region, Salesforce recommends that you include our current IP address ranges for regions where you have end users. If you use client-side certificate pinning to validate the server's certificate, Salesforce doesn't recommend pinning leaf certificates. Because Salesforce Edge Network uses data center specific certificates, Salesforce recommends that you pin the intermediate certificate instead for a better experience.

1. From Setup, in the Quick Find box, enter *My Domain*, and then select **My Domain**.
2. Under Routing and Policies, select **Edit**.
3. Select **Use Salesforce Edge Network**, and save your changes.

 **Important:** Salesforce Edge Network can be disabled by Salesforce Customer Support.

To avoid potential conflicts between follow-up processes such as CNAME and DNS updates, you can't make a change that requires provisioning for 15 minutes after you move to Salesforce Edge Network. Changes that require provisioning include changing your My Domain name or suffix, enabling enhanced domains, and removing a previous My Domain name.

Routing applies to most provisioned and deployed domains for this org. For details, see Considerations for Salesforce Edge Network. To maximize the number of URLs that are routed through Salesforce Edge Network, enable enhanced domains.

SEE ALSO:

[My Domain](#)

[Knowledge Article: Salesforce IP Addresses and Domains to Allow](#)

[Considerations for Salesforce Edge Network](#)

[Enhanced Domains](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To edit My Domain settings:

- Customize Application

Get Your Org Status and Upcoming Maintenance Dates with My Domain

Get information about system performance and availability from `trust.salesforce.com`. This trust page reports status information based on your Salesforce instance. If you don't know your instance, use your My Domain name to look it up.

1. Go to [Trust Status](#).

The Status page shows any current incidents and provides quick access to recently viewed instances.

2. To view information for your instance, enter your My Domain name in the search bar.

Don't enter your complete login URL. You can get your My Domain name from the My Domain Setup page or via the subdomain for your My Domain login URL. For example, if your org's My Domain login URL is `https://example.my.salesforce.com`, enter `example`.

Tip: If you don't want to use your My Domain name, you can find your instance on the Company Information Setup page. From Setup, in the Quick Find box, enter *Company Information*, and then select **Company Information**. The Instance field contains your Salesforce instance.

3. Under My Domains, select your instance.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

The screenshot displays the Salesforce Trust Status interface. At the top, there's a search bar and navigation icons. The main header shows the instance name 'MYCOMPANY | AP17'. A 'CURRENT STATUS' tab is highlighted with a red box and a '1' callout. Below it, a green bar indicates the 'OVERALL SYSTEM' status is 'Available'. A table lists various services with green checkmarks, indicating they are all operational. On the right, the 'Instance Details' sidebar (callout '2') provides specific information: Version Summer '22 Patch 18.14, Region Asia Pacific, and Maintenance Window Saturdays 15:00 - 19:00 UTC. A 'Subscribe' button (callout '3') is located in the top right corner.

The Current Status (1) displays by default. In the Instance Details section (2), you can find your current version, region, and maintenance window. To subscribe to updates, click **Subscribe** (3). For more information on subscriptions, see the [Trust Status Notification Guide](#).

Here are the possible color indicators for your status.

- Green (Available): This instance is available and fully functional.
- Blue (Informational): Used to display information about the instance that's unrelated to a performance issue or service disruption.

- Purple (Maintenance): This instance is in maintenance. An informational message indicates your ability to access the instance during the maintenance.
- Yellow (Service Degradation): The instance is accessible, but some functionality is unavailable or the service is running with significant latency. To get more information, click the incident number.
- Red (Service Disruption): The instance is inaccessible to customers. To get more information, click the incident number.

4. To get a historical view of your status, click **History**.

The screenshot shows the Salesforce Trust | Status interface. The 'History' tab is selected and highlighted with an orange box. The main content area displays a timeline of service status for various products from 9/6 to NOW. All services shown (Core Service, Search, Analytics, Live Agent, CPQ and Billing) have green bars and checkmarks, indicating they are operational. The right sidebar shows Instance Details including Version (Summer '22 Patch 18.14), Region (Asia Pacific), and Maintenance Window (Saturdays 15:00 - 19:00 UTC).

Optionally, you can select a range and enter a date around which to center the range. For example, to view your history from August 29, 2022 to September 4, 2022, select **7Days**, and then select September 1, 2022 as the date.

5. To view maintenance events, click **Maintenance**.

The screenshot shows the Salesforce Maintenance page for instance MYCOMPANY | AP17. The page has a navigation bar with 'Trust | Status' and a search bar. Below the navigation bar, there are tabs for 'CURRENT STATUS', 'HISTORY', and 'MAINTENANCE'. The 'MAINTENANCE' tab is selected and highlighted with a red box labeled '1'. Below the tabs, there is a table of maintenance events. The table has columns for ID, DATE, START TIME, SUBJECT, INSTANCES, SERVICES, and TYPE. The table is filtered to show events from 9/8/22 to 12/31/23. A red box labeled '2' highlights the 'PAST 33 DAYS (1)' link at the top of the table. The table shows several events, with the row for the 'Winter '23 Major Release' event on October 15 highlighted with a red box labeled '3'. The event details are: ID 514589, DATE Oct 15, START TIME 11:00 am MDT, SUBJECT Winter '23 Major Release, INSTANCES AP17, SERVICES Core Service, and TYPE Release. To the right of the table, there is an 'Instance Details' section with information about the version, region, and maintenance window.

After you click **Maintenance** (1), you can view 12 months of future maintenance events. If maintenance events occurred within the past 33 days, a link with a count is available at the top of the list (2). To display those events in the table, click **PAST 33 DAYS (#)**. In this example, AP17 is scheduled to get the Winter '23 Major Release on October 15 (3). For more details on a maintenance event, click the ID number.

 **Note:** The Instance Details section includes your standard maintenance window in the UTC time zone. The date and time for maintenance events are in the user's time zone, as detected by the browser.

SEE ALSO:

[My Domain](#)

Link to Salesforce Domains in Packages

If you provide a package to Salesforce customers through AppExchange, review your code for hard-coded URLs and code that parses a known URL. The URLs that Salesforce serves for a target org vary based on the org type and configuration. Hard-coded URLs and code that assumes the format of a URL can break when a customer enables enhanced domains, enables partitioned domains, or changes their My Domain name. Also, URL formats can vary between production orgs, sandboxes, and other non-production orgs. To ensure that your package functionality continues to work with all possible URL formats, update hard-coded URL references to relative URLs whenever possible. When a relative URL isn't possible, use a dynamically generated hostname.

To build packages that support all possible URL formats, check your package for hard-coded URLs. For example, a link to embedded content on a Visualforce page or a button that calls a Visualforce page. If the link includes a URL in plain text, the corresponding functionality can break when enhanced domains or partitioned domains are enabled. To find hard-coded URLs in your package, search your code for the domain suffixes on [My Domain URL Format Changes When You Enable Enhanced Domains](#) in Salesforce Help.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

If you find a hard-coded URL, we recommend that you replace it with a relative URL whenever possible. For example, to create a link from one Visualforce page to another, use the path without the `*.com` hostname. If your package functionality requires a full hostname, use the Apex `System.DomainCreator` class to get the corresponding hostnames. With this method, your package works in all orgs, regardless of the org type, My Domain settings, and whether enhanced domains are enabled. For more information, see [Call Salesforce URLs Within a Package](#) in the *First-Generation Managed Packaging Developer Guide*.

If you find code in your package that parses a known URL or domain to get a value, we recommend that you update that code to use the `System.DomainParser` and `System.Domain` Apex classes. For more information, see [Call Salesforce URLs Within a Package](#) in the *First-Generation Managed Packaging Developer Guide*.

Deliver and Communicate Updates

If your package requires updates, we recommend that you offer those fixes in a minor or patch release if possible. Customers are more likely to adopt a minor or patch release, rather than a major release. Also, because customers often remain on the major release that they initially installed, consider offering a minor or patch release for each major release in the field.

To help your customers plan, clearly communicate which versions of your package support enhanced domains and partitioned domains. Also specify any prior major versions for which you can't offer support for those features.

SEE ALSO:

[My Domain](#)

[Enhanced Domains](#)

[Partitioned Domains](#)

Log In to Salesforce with Code

For an extra layer of security, use your My Domain login URL to access your Salesforce org with code. Compare the benefits of your My Domain login URL versus the default Salesforce login URL. And understand why we don't recommend that you use URLs that contain your Salesforce instance.

You have three options to log in to Salesforce with code such as API calls and Apex code.

- Your My Domain login URL, in the format `https://MyDomainName.my.salesforce.com` for production orgs and `https://MyDomainName--SandboxName.sandbox.my.salesforce.com` for sandboxes with enhanced domains.
- The default Salesforce login URLs: `https://login.salesforce.com` for production and Developer Edition orgs and `https://test.salesforce.com` for sandboxes.
- Your org's instanced URL in the format `https://InstanceName.salesforce.com`. For example, `https://na139.salesforce.com`.

You can choose which option to use, or you can use more than one option. For example, you can use your My Domain login URL for all new code while still using default login URLs in your existing code. To prevent issues when your org's instance changes, we recommend that you replace all instanced URLs in your code.

 **Tip:** To search your Salesforce code, download the metadata. Then use a command-line interface, such as [Salesforce CLI](#).

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

Recommended: Your My Domain Login URL

Your My Domain login URL contains your company-specific My Domain name. Because My Domain names are unique, using your My Domain login URL adds another layer of security.

Admins can require SOAP API calls to log in using the org's My Domain login URL via a My Domain setting. Also, this login URL continues to work when your org is moved to another instance.

For these reasons, we recommend that you use your My Domain login URL to access your org with code.

There's one consideration for using your My Domain login URL with code. If you rename your My Domain, for example, when your brand or company name changes, your My Domain login URL changes. In this situation, your code breaks until you update the references to the previous My Domain login URL in your code.

For API integrations, use the `metadataServerUrl` or `serverURL` value returned by a [login request](#). To get the hostname of your My Domain login URL in Apex, use the `getOrgMyDomainHostname()` method of the `System.DomainCreator` class. These methods continue to work after a My Domain change.

Default Salesforce Login URLs

The default login URLs of `https://login.salesforce.com` for production and Developer Edition orgs and `https://test.salesforce.com` for sandboxes work well in code. These URLs continue to work when your org is moved to another instance and when you rename your My Domain.

However, these default login URLs don't have the extra layer of security of including your company-specific My Domain name. Also, an admin can require SOAP API calls to log in using the org's My Domain login URL via a My Domain setting. When that setting is enabled, these default login URLs don't work in SOAP API calls.

Instanced Salesforce URLs

We don't recommend instanced URLs when logging in to Salesforce with code or as a user. When your org is moved to another Salesforce instance, code using the instanced URL breaks. If you find instanced URLs in your code, replace them with your My Domain login URL or the default Salesforce login URL.

SEE ALSO:

[My Domain](#)

[Apex Reference Guide: DomainCreator Class](#)

[Set the My Domain Login Policy](#)

My Domain URL Formats

Your My Domain name is a subdomain used in login URL and application URLs across your Salesforce org, including sites and Visualforce pages. Understand what determines your org's URL formats and the structure of those formats.

All orgs get a My Domain by default. If you don't like your org's My Domain name, you can change it.

A My Domain uses Salesforce domain suffixes such as `my.salesforce.com` for your org's URLs. With enhanced domains, your My Domain name is used in the system-managed hostnames for you Salesforce Sites and Experience Cloud sites. To use a custom domain such as `https://www.example.com` to serve your org's Salesforce Sites and Experience Cloud sites, see [Custom Domains](#).

[What Determines Your URL Formats](#)

Understand how your My Domain affects the login and application URLs for your Salesforce org, and learn about enhanced domains. Review the impact of stabilizing certain URL formats when you have a My Domain.

[My Domain Hostnames](#)

Understand the purpose of each hostname that Salesforce serves for your org.

[My Domain Login and Application URL Formats with Enhanced Domains](#)

Review the login and application URL formats for Salesforce orgs. The URLs are different for production and sandbox orgs.

[My Domain Login and Application URL Formats Without Enhanced Domains](#)

Review the URL formats that Salesforce served for Salesforce orgs without enhanced domains. The URLs are different for production and sandbox orgs.

[My Domain URL Format Changes When You Enable Enhanced Domains](#)

Understand how login and application URL formats changed when you deploy enhanced domains.

SEE ALSO:

[My Domain](#)

[Change Your My Domain Details](#)

[Update Your Org and Test My Domain Changes](#)

What Determines Your URL Formats

Understand how your My Domain affects the login and application URLs for your Salesforce org, and learn about enhanced domains. Review the impact of stabilizing certain URL formats when you have a My Domain.

My Domain provides a customer-specific login URL for your Salesforce org and updates your Visualforce, Experience Builder, and content URLs.

 **Note:** All orgs get a My Domain by default. If you don't like your My Domain name or circumstances warrant a change, you can rename it.

The My Domain format of the login URL for a production org is

MyDomainName.my.salesforce.com. You can also allow users to continue to log in from

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

`login.salesforce.com`. With enhanced domains, which were enforced in Winter '24, Salesforce application URLs also contain your My Domain name as a subdomain and URLs for sandboxes use a different format.

For non-production orgs other than sandboxes, the URL formats differ based on whether partitioned domains are enabled. Qualifying new orgs get this feature by default. With partitioned domains, the My Domain URL formats include a word related to the org type.

Partitioned Domains

With partitioned domains, My Domain hostnames for your non-production org include a word related to the org type. For example, partitioned domains for Developer Edition orgs include the word `develop`. Partitioned domains allow Salesforce to maximize the availability of your orgs by gradually rolling out delivery changes. And it's easier to identify an org by a URL when the domain is partitioned.

Qualifying new non-production orgs are partitioned by default, and you can't disable partitioning in those orgs.

For more information and lists of the URL formats for these org types, see [Partitioned Domains](#).

Enhanced Domains

Enhanced domains are the current version of My Domain that meets the latest browser requirements. In Winter '24, all orgs got enhanced domains and the feature can't be disabled.

With enhanced domains, all URLs across your org contain your company-specific My Domain name, including URLs for your Experience Cloud sites, Salesforce Sites, Visualforce pages, and content files. These URLs also comply with the latest browser requirements, allowing your users to access Salesforce using browsers that block third-party cookies.

All application URLs start with your org's My Domain name and no application URLs contain your instance name. Also, sandbox org URLs include the word "sandbox," making it easy to identify a sandbox org from its URL. With no instance names, enhanced My Domain URLs are easier for users to remember and remain stabilized when your org is moved to another Salesforce instance.

If your org was created before Summer '22, enhanced domains weren't enabled by default. When enhanced domains were deployed, the domain suffix—the part after the My Domain name—changed for Experience Cloud sites, Salesforce Sites, content files, Site.com Studio, Experience Builder, and Visualforce URLs.

Before enhanced domains were deployed, the formats for several other URLs varied based on the My Domain setting: **Stabilize URLs for Visualforce, Experience Builder, Site.com Studio, and content files**.

For a full list of the legacy URL formats for an org without enhanced domains, see [My Domain Login and Application URL Formats Without Enhanced Domains](#).

For a full list of URL formats that changed when enhanced domains were deployed, see [My Domain URL Format Changes When You Enable Enhanced Domains](#).

SEE ALSO:

[My Domain](#)

[My Domain Login and Application URL Formats with Enhanced Domains](#)

[My Domain Login and Application URL Formats Without Enhanced Domains](#)

[Custom Domains](#)

My Domain Hostnames

Understand the purpose of each hostname that Salesforce serves for your org.

For the format of these hostnames, see My Domain URL Formats in Salesforce Help.

Hostname Type	Use
Login	Salesforce login authentication. For example, sales reps, support agents, and admins log in to MyDomainName.my.salesforce.com . API calls and third-party integrations can also use this hostname for authentication.
Application Page or Tab	The URL for a Salesforce Classic page or tab served by Salesforce to authenticated users. This URL uses the login hostname plus an identifier in the format MyDomainName.my.salesforce.com/PageID .
Content (files)	Files stored in Salesforce. For example, images or files served outside of an Experience Cloud site or Salesforce Site.
Content Management System (CMS) public channels	Public-facing channels that let you share the content in your CMS Workspaces with one or more endpoints, or channels. For example, you can share your content in marketing emails, websites, or custom apps. For more information, see Salesforce CMS .
Email tracking	The sfdcopens.com domain is reserved for future use with email tracking.
Experience Cloud sites	When Digital Experiences are enabled and configured, this hostname serves your public-facing Experience Cloud sites. For more information, see Experience Cloud .
Experience Builder	When Digital Experiences are enabled, admins use Experience Builder to customize Experience Cloud sites. For example, they can add company branding, share Salesforce records with site members, and work with them in a collaborative space that meets your needs. For more information, see Build and Customize Your Experience Cloud Site .
Experience Builder Preview	When Digital Experiences are enabled, admins use Experience Builder to customize Experience Cloud sites. If the site or its changes aren't published, users can preview the site from Experience Builder as an authenticated user or guest user. This hostname serves the preview in the new tab. Within Experience Builder in Preview mode, certain features aren't available in their entirety. For more information, see Build and Customize Your Experience Cloud Site .
Experience Builder Live Preview	When Digital Experiences are enabled, admins use Experience Builder to customize Experience Cloud sites. When a user previews a site within Experience Builder, this hostname serves the preview. For more information, see Build and Customize Your Experience Cloud Site .
Lightning	Lightning pages served by Salesforce to authenticated users. For example, MyDomainName.lightning.force.com/lightning/page/home .

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Hostname Type	Use
Lightning Container Component	In Aura, the <code>lightning:container</code> component hosts content in an iframe. This hostname serves that content. For more information, see Lightning Container in the Lightning Aura Components Developer Guide.
Salesforce Sites	Salesforce Sites are public websites and applications that are directly integrated with your Salesforce org—without requiring users to log in with a username and password. For more information, see Salesforce Sites .
Setup Pages	The <code>salesforce-setup.com</code> domain hosts Setup pages in Salesforce.
Next generation Omni-Channel engagement (examples: voice and messaging)	The hostname that serves content through Service Cloud Voice and Service Cloud Messaging. For more information, see Service Cloud Voice and Messaging in Service Cloud .
User Content and Images	Content from a third party displayed in Salesforce via an inline frame (iframe). For example, Google Maps displayed within an iframe next to an address field.
User Content on a Government Cloud org	Within a Government Cloud org, content from a third party displayed in Salesforce via an inline frame (iframe). User content stored in a Salesforce Government Cloud org. For example, Google Maps displayed within an iframe next to an address field.
Visualforce	Visualforce pages, the top-level container for custom apps built with Visualforce. For more information, see the Visualforce Developer Guide .

SEE ALSO:

[My Domain URL Formats](#)

My Domain Login and Application URL Formats with Enhanced Domains

Review the login and application URL formats for Salesforce orgs. The URLs are different for production and sandbox orgs.

Enhanced domains are the current version of My Domain that meets the latest browser requirements.

If your org was created before Summer '22, enhanced domains weren't enabled by default. To understand the impact to your org when enhanced domains were deployed, see [My Domain URL Format Changes When You Enable Enhanced Domains](#).

To better understand the purpose of each hostname and whether it applies to you, see [My Domain Hostnames](#).

My Domain URL Formats for Production Orgs

 **Note:** If you deploy a My Domain in a Developer Edition org, the My Domain name ends in `-dev-ed`. For example: `https://example-dev-ed.my.salesforce.com`.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

URL TYPE	URL FORMAT
Login	<i>MyDomainName</i> .my.salesforce.com
Application Page or Tab	<i>MyDomainName</i> .my.salesforce.com/ <i>PageID</i>

URL TYPE	URL FORMAT
Content (files)	MyDomainName .file.force.com
Content Management System (CMS) public channels	MyDomainName .cdn.salesforce-experience.com
Email tracking (reserved for future use)	MyDomainName .my.sfdcopens.com
Experience Cloud sites	MyDomainName .my.site.com
Experience Builder	MyDomainName .builder.salesforce-experience.com
Experience Builder Preview	MyDomainName .preview.salesforce-experience.com
Experience Builder Live Preview	MyDomainName .live-preview.salesforce-experience.com
Lightning	MyDomainName .lightning.force.com
Lightning Container Component	MyDomainName -- PackageName .container.force.com ¹
Salesforce Sites	MyDomainName .my.salesforce-sites.com
Setup Pages	MyDomainName .my.salesforce-setup.com
Next generation Omni-Channel engagement (examples: voice and messaging)	MyDomainName .my.salesforce-scrt.com
User Content	MyDomainName -- UniqueID .my.force-user-content.com
User Content on a Government Cloud org	MyDomainName -- UniqueID .gia.force-user-content.com
User Image (reserved for future use)	MyDomainName -- UniqueID .file.force-user-content.com
Visualforce	MyDomainName -- PackageName .vf.force.com ¹

¹ If your installed package is unmanaged, the package name is c.

My Domain URL Formats for Sandbox Orgs

URL TYPE	URL FORMAT
Login	MyDomainName -- SandboxName .sandbox.my.salesforce.com
Application Page or Tab	MyDomainName -- SandboxName .sandbox.my.salesforce.com/ PageID

URL TYPE	URL FORMAT
Content (files)	MyDomainName--SandboxName .sandbox.file.force.com
Content Management System (CMS) public channels	MyDomainName--SandboxName .sandbox.cdn.salesforce-experience.com
Email tracking (reserved for future use)	MyDomainName--SandboxName .sandbox.my.sfdcopens.com
Experience Cloud Sites	MyDomainName--SandboxName .sandbox.my.site.com
Experience Builder	MyDomainName--SandboxName .sandbox.builder.salesforce-experience.com
Experience Builder Preview	MyDomainName--SandboxName .sandbox.preview.salesforce-experience.com
Experience Builder Live Preview	MyDomainName--SandboxName .sandbox.live-preview.salesforce-experience.com
Lightning	MyDomainName--SandboxName .sandbox.lightning.force.com
Lightning Container Component	MyDomainName--SandboxName--PackageName .sandbox.container.force.com ¹
Salesforce Sites	MyDomainName--SandboxName .sandbox.my.salesforce-sites.com
Setup Pages	MyDomainName--SandboxName .sandbox.my.salesforce-setup.com
Next generation Omni-Channel engagement (examples: voice and messaging)	MyDomainName--SandboxName .sandbox.my.salesforce-scrt.com
User Content	MyDomainName--SandboxName--UniqueID .sandbox.my.force-user-content.com
User Content on a Government Cloud org	MyDomainName--SandboxName--UniqueID .sandbox.gia.force-user-content.com
User Image (reserved for future use)	MyDomainName--SandboxName--UniqueID .sandbox.file.force-user-content.com
Visualforce	MyDomainName--SandboxName--PackageName .sandbox.vf.force.com ¹

¹ If your installed package is unmanaged, the package name is `c`.

SEE ALSO:

- [What Determines Your URL Formats](#)
- [Update Your Org for My Domain Changes](#)
- [Custom Domains](#)

My Domain Login and Application URL Formats Without Enhanced Domains

Review the URL formats that Salesforce served for Salesforce orgs without enhanced domains. The URLs are different for production and sandbox orgs.

 **Note:** Enhanced domains are the current version of My Domain that meets the latest browser requirements. In Winter '24, all orgs got enhanced domains and the feature can't be disabled. For the current My Domain formats, see [My Domain Login and Application URL Formats with Enhanced Domains](#).

In an org without enhanced domains, your My Domain name wasn't used in Salesforce Sites and Experience Cloud sites URLs. The default URL formats for Salesforce Sites and Experience Cloud sites are listed in these tables for reference. To use a custom domain such as `https://www.example.com` to serve your org's Salesforce sites and Experience Cloud sites, see [Custom Domains](#).

To better understand the purpose of each My Domain type and whether it applies to you, see [My Domain Hostnames](#) in Salesforce Help.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

My Domain URL Formats for Production Orgs

 **Note:** If you deploy a My Domain in a Developer Edition org, the My Domain name ends in `-dev-ed`. For example: `https://example-dev-ed.my.salesforce.com`.

URL TYPE	URL FORMAT
Login	<i>MyDomainName</i> .my.salesforce.com
Application Page or Tab	<i>MyDomainName</i> .my.salesforce.com/ <i>PageID</i>
Experience Cloud Sites	<i>ExperienceCloudSitesSubdomainName</i> .force.com
Lightning	<i>MyDomainName</i> .lightning.force.com
Lightning Container Component	<i>MyDomainName--PackageName</i> .container.lightning.com ¹
Salesforce Sites	<i>SitesSubdomainName</i> .secure.force.com
Salesforce Sites (HTTP Only)	<i>SitesSubdomainName</i> .force.com
Next generation Omni-Channel engagement (examples: voice and messaging)	<i>Region</i> .s crt.sfdc.sh

URL TYPE	URL FORMAT
User Content	<i>MyDomainName--UniqueID.a.forceusercontent.com</i>
User Content on a Government Cloud org	<i>MyDomainName--UniqueID.c.forceusercontent.com</i>
User Image (reserved for future use)	<i>MyDomainName--UniqueID.d.forceusercontent.com</i>

If the Stabilize URLs for Visualforce, Experience Builder, Site.com Studio, and content files setting is enabled, these URL formats apply to your org.

URL TYPE	URL FORMAT
Content (files)	<i>MyDomainName--c.documentforce.com</i>
Experience Builder	<i>MyDomainName.builder.salesforce-communities.com</i>
Experience Builder Preview	<i>MyDomainName.preview.salesforce-communities.com</i>
Experience Builder Live Preview	<i>MyDomainName.livepreview.salesforce-communities.com</i>
Visualforce	<i>MyDomainName--PackageName.visualforce.com</i> ¹

If the Stabilize URLs for Visualforce, Experience Builder, Site.com Studio, and content files setting isn't enabled, these URL formats apply to your org.

URL TYPE	URL FORMAT
Content (files) in a non-Hyperforce org	<i>MyDomainName--c.InstanceName.content.force.com</i>
Content (files) in a Hyperforce org	<i>MyDomainName--c.InstanceName.content.sfdc-HyperforceInstanceName.force.com</i>
Experience Builder in a non-Hyperforce org	<i>MyDomainName--sitestudio.InstanceName.force.com</i>
Experience Builder in a Hyperforce org	<i>MyDomainName--sitestudio.InstanceName.sfdc-HyperforceInstanceName.force.com</i>
Experience Builder Preview in a non-Hyperforce org	<i>MyDomainName--sitepreview.InstanceName.force.com</i>
Experience Builder Preview in a Hyperforce org	<i>MyDomainName--sitepreview.InstanceName.sfdc-HyperforceInstanceName.force.com</i>

URL TYPE	URL FORMAT
Experience Builder Live Preview in a non-Hyperforce org	MyDomainName --livepreview. InstanceName .force.com
Experience Builder Live Preview in a Hyperforce org	MyDomainName --livepreview. InstanceName .sfdc- HyperforceInstanceName .force.com
Visualforce in a non-Hyperforce org	MyDomainName -- PackageName . InstanceName .visual.force.com ¹
Visualforce in a Hyperforce org	MyDomainName -- PackageName . InstanceName .visual.sfdc- HyperforceInstanceName .force.com ¹

¹ If your installed package is unmanaged, the package name is c.

My Domain URL Formats for Sandbox Orgs

URL TYPE	URL FORMAT
Login	MyDomainName -- SandboxName .my.salesforce.com
Application Page or Tab	MyDomainName -- SandboxName .my.salesforce.com/ PageID
Experience Cloud Sites	SandboxName - ExperienceCloudSitesSubdomainName . InstanceName .force.com
Lightning	MyDomainName -- SandboxName .lightning.force.com
Lightning Container Component	MyDomainName -- SandboxName -- PackageName .container.lightning.com ¹
Salesforce Sites	SandboxName - SitesSubdomainName . InstanceName .force.com
Next generation Omni-Channel engagement (examples: voice and messaging)	Region .s crt.sfdc.sh
User Content	MyDomainName -- SandboxName -- UniqueID .b.forceusercontent.com
User Content on a Government Cloud org	MyDomainName -- SandboxName -- UniqueID .c.forceusercontent.com
User Image (reserved for future use)	MyDomainName -- SandboxName -- UniqueID .d.forceusercontent.com

If the Stabilize URLs for Visualforce, Experience Builder, Site.com Studio, and content files setting is enabled, these URL formats apply to your org.

URL TYPE	URL FORMAT
Content (files)	MyDomainName--SandboxName--c.documentforce.com
Experience Builder	MyDomainName--SandboxName.builder.salesforce-communities.com
Experience Builder Preview	MyDomainName--SandboxName.preview.salesforce-communities.com
Experience Builder Live Preview	MyDomainName--SandboxName.livepreview.salesforce-communities.com
Visualforce	MyDomainName--SandboxName--PackageName.visualforce.com¹

If the Stabilize URLs for Visualforce, Experience Builder, Site.com Studio, and content files setting isn't enabled, these URL formats apply to your org.

URL TYPE	URL FORMAT
Content (files) in a non-Hyperforce org	MyDomainName--SandboxName--c.InstanceName.content.force.com
Content (files) in a Hyperforce org	MyDomainName--SandboxName--c.InstanceName.content.sfdc-HyperforceInstanceName.force.com
Experience Builder in a non-Hyperforce org	MyDomainName--SandboxName--sitestudio.InstanceName.force.com
Experience Builder in a Hyperforce org	MyDomainName--SandboxName--sitestudio.InstanceName.sfdc-HyperforceInstanceName.force.com
Experience Builder Preview in a non-Hyperforce org	MyDomainName--SandboxName--sitepreview.InstanceName.force.com
Experience Builder Preview in a Hyperforce org	MyDomainName--SandboxName--sitepreview.InstanceName.sfdc-HyperforceInstanceName.force.com
Experience Builder Live Preview in a non-Hyperforce org	MyDomainName--SandboxName--livepreview.InstanceName.force.com
Experience Builder Live Preview in a Hyperforce org	MyDomainName--SandboxName--livepreview.InstanceName.sfdc-HyperforceInstanceName.force.com
Visualforce in a non-Hyperforce org	MyDomainName--SandboxName--PackageName.InstanceName.visual.force.com¹
Visualforce in a Hyperforce org	MyDomainName--SandboxName--PackageName.InstanceName.visual.sfdc-HyperforceInstanceName.force.com¹

¹ If your installed package is unmanaged, the package name is `c`.

SEE ALSO:

[My Domain](#)

[What Determines Your URL Formats](#)

[Update Your Org for My Domain Changes](#)

[Custom Domains](#)

My Domain URL Format Changes When You Enable Enhanced Domains

Understand how login and application URL formats changed when you deploy enhanced domains.

Enhanced domains are the current version of My Domain that meets the latest browser requirements. The feature is enforced and you can't disable it. The information in this topic is designed to assist customers in testing for the end of non-enhanced redirections in Winter '25.

With enhanced domains, all application URLs start with your org's My Domain name. When enhanced domains were deployed, instance names were removed from all My Domain URLs, and package names were removed from some URLs. With no instance names, enhanced My Domain URLs are easier for users to remember and remain stabilized when your org is moved to another Salesforce instance.

To better understand the purpose of each hostname type and whether it applies to you, see [My Domain Hostnames](#) in Salesforce Help.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Production Org URL Format Changes

These URL formats change when you enable and deploy enhanced domains in a production org.

 **Note:** If you deploy a My Domain in a Developer Edition org, the My Domain name ends in `-dev-ed`. For example: `https://example-dev-ed.my.salesforce.com`.

URL TYPE	FORMAT	URL FORMAT
Login	Old	<i>MyDomainName</i> .my.salesforce.com
	New	This URL doesn't change when you enable and deploy enhanced domains unless you also change your My Domain name or suffix.
Application Page or Tab	Old	<i>MyDomainName</i> .my.salesforce.com/ <i>pageID</i>
	New	This URL doesn't change when you enable and deploy enhanced domains unless you also change your My Domain name or suffix.
Content Management System (CMS) public channels	Old	<i>MyDomainName</i> .cdn.salesforce-experience.com
	New	This URL doesn't change when you enable and deploy enhanced domains unless you also change your My Domain name or suffix.
Email tracking (reserved for future use)	Old	<i>MyDomainName</i> .my.sfdcopens.com
	New	This URL is reserved for future use. No related updates are required after you enable and deploy enhanced domains.

URL TYPE	FORMAT	URL FORMAT
Lightning	Old	MyDomainName .lightning.force.com
	New	This URL doesn't change when you enable and deploy enhanced domains unless you also change your My Domain name or suffix.
Experience Cloud sites	Old	ExperienceCloudSitesSubdomainName .force.com
	New	MyDomainName .my.site.com
Lightning Container Component	Old	MyDomainName--PackageName .container.lightning.com ¹
	New	MyDomainName--PackageName .container.force.com ¹
Salesforce Sites	Old	SitesSubdomainName .secure.force.com
	New	MyDomainName .my.salesforce-sites.com
Salesforce Sites (HTTP only)	Old	SitesSubdomainName .force.com
	New	MyDomainName .my.salesforce-sites.com
Setup Pages	Old	This URL requires enhanced domains. No related updates are required after you enable and deploy enhanced domains.
	New	MyDomainName .my.salesforce-setup.com
Service Cloud Real-Time	Old	LiveAgentPool .salesforceliveagent.com
	New	This URL doesn't change when you enable and deploy enhanced domains.
Next generation Omni-Channel engagement (examples: voice and messaging)	Old	MyDomainName .my.salesforce-scrt.com
	New	This URL doesn't change when you enable and deploy enhanced domains unless you also change your My Domain name or suffix.
User Content	Old	MyDomainName--UniqueID .a.forceusercontent.com
	New	MyDomainName--UniqueID .my.force-user-content.com
User Content on a Government Cloud org	Old	MyDomainName--UniqueID .c.my.force-user-content.com
	New	MyDomainName--UniqueID .gia.force-user-content.com
User Image (reserved for future use)	Old	MyDomainName--UniqueID .file.force-user-content.com
	New	This URL is reserved for future use. No related updates are required after you enable and deploy enhanced domains.

If the **Stabilize URLs for Visualforce, Experience Builder, Site.com Studio, and content files** setting is enabled before you enable and deploy enhanced domains, these production formats change.

URL TYPE	FORMAT	URL FORMAT
Content (Files)	Old	MyDomainName--c .documentforce.com

URL TYPE	FORMAT	URL FORMAT
	New	MyDomainName .file.force.com
Experience Builder	Old	MyDomainName .builder.salesforce-communities.com
	New	MyDomainName .builder.salesforce-experience.com
Experience Builder Live Preview	Old	MyDomainName .livepreview.salesforce-communities.com
	New	MyDomainName .live-preview.salesforce-experience.com
Experience Builder Preview	Old	MyDomainName .preview.salesforce-communities.com
	New	MyDomainName .preview.salesforce-experience.com
Visualforce	Old	MyDomainName--PackageName .visualforce.com ¹
	New	MyDomainName--PackageName .vf.force.com ¹

If the **Stabilize URLs for Visualforce, Experience Builder, Site.com Studio, and content files** setting isn't enabled before you enable and deploy enhanced domains, these production URL formats change.

URL TYPE	FORMAT	URL FORMAT
Content (Files) in a non-Hyperforce org	Old	MyDomainName--c.InstanceName .content.force.com
	New	MyDomainName .file.force.com
Content (Files) in a Hyperforce org	Old	MyDomainName--c.InstanceName .content.sfdc- HyperforceInstanceName .force.com
	New	MyDomainName .file.force.com
Experience Builder in a non-Hyperforce org	Old	MyDomainName--sitestudio.InstanceName .force.com
	New	MyDomainName .builder.salesforce-experience.com
Experience Builder in a Hyperforce org	Old	MyDomainName--sitestudio.InstanceName .sfdc- HyperforceInstanceName .force.com
	New	MyDomainName .builder.salesforce-experience.com
Experience Builder Live Preview in a non-Hyperforce org	Old	MyDomainName--livepreview.InstanceName .force.com
	New	MyDomainName .live-preview.salesforce-experience.com
Experience Builder Live Preview in a Hyperforce org	Old	MyDomainName--livepreview.InstanceName .sfdc- HyperforceInstanceName .force.com
	New	MyDomainName .live-preview.salesforce-experience.com
Experience Builder Preview in a non-Hyperforce org	Old	MyDomainName--sitepreview.InstanceName .force.com
	New	MyDomainName .preview.salesforce-experience.com
Experience Builder Preview in a Hyperforce org	Old	MyDomainName--sitepreview.InstanceName .sfdc- HyperforceInstanceName .force.com
	New	MyDomainName .preview.salesforce-experience.com

URL TYPE	FORMAT	URL FORMAT
Visualforce in a non-Hyperforce org	Old	MyDomainName--PackageName.InstanceName .visual.force.com ¹
	New	MyDomainName--PackageName .vf.force.com ¹
Visualforce in a Hyperforce org in a Hyperforce org	Old	MyDomainName--PackageName.InstanceName .visual.sfdc- HyperforceInstanceName .force.com ¹
	New	MyDomainName--PackageName .vf.force.com ¹

¹ If your installed package is unmanaged, the package name is c.

Sandbox Org URL Format Changes

These URL formats change when you enable and deploy enhanced domains in a sandbox.

URL TYPE	FORMAT	URL FORMAT
Login	Old	MyDomainName--SandboxName .my.salesforce.com
	New	MyDomainName--SandboxName .sandbox.my.salesforce.com
Application Page or Tab	Old	MyDomainName--SandboxName .my.salesforce.com/ PageID
	New	MyDomainName--SandboxName .sandbox.my.salesforce.com/ PageID
Email tracking (reserved for future use)	Old	MyDomainName--SandboxName .sandbox.my.sfdcopens.com
	New	This URL is reserved for future use. No related updates are required after you enable and deploy enhanced domains.
Experience Cloud sites	Old	SandboxName-ExperienceCloudSitesSubdomainName . InstanceName .force.com
	New	MyDomainName--SandboxName .sandbox.my.site.com
My Domain Login (old format)	Old	MyDomainName--SandboxName.InstanceName .my.salesforce.com
	New	MyDomainName--SandboxName .sandbox.my.salesforce.com
Lightning	Old	MyDomainName--SandboxName .lightning.force.com
	New	MyDomainName--SandboxName .sandbox.lightning.force.com
Lightning Container Component	Old	MyDomainName--SandboxName--PackageName .container.lightning.com ¹
	New	MyDomainName--SandboxName--PackageName .sandbox.container.force.com ¹
Salesforce Sites	Old	SandboxName-SitesSubdomainName . InstanceName .force.com
	New	MyDomainName--SandboxName .sandbox.my.salesforce-sites.com
Setup Pages	Old	This URL requires enhanced domains. No related updates are required after you enable and deploy enhanced domains.
	New	MyDomainName--SandboxName .sandbox.my.salesforce-setup.com
Service Cloud Real-Time	Old	LiveAgentPool .salesforceliveagent.com

URL TYPE	FORMAT	URL FORMAT
	New	This URL doesn't change when you enable and deploy enhanced domains.
Next generation Omni-Channel engagement (examples: voice and messaging)	Old	MyDomainName--SandboxName .my.salesforce-scrt.com
	New	MyDomainName--SandboxName .sandbox.my.salesforce-scrt.com
User Content	Old	MyDomainName--SandboxName--UniqueID .b.forceusercontent.com
	New	MyDomainName--SandboxName--UniqueID .sandbox.my.force-user-content.com
User Content on a Government Cloud org	Old	MyDomainName--SandboxName--UniqueID .c.forceusercontent.com
	New	MyDomainName--SandboxName--UniqueID .sandbox.gia.force-user-content.com
User Image (reserved for future use)	Old	MyDomainName--SandboxName--UniqueID .sandbox.file.force-user-content.com
	New	This URL is reserved for future use. No related updates are required after you enable and deploy enhanced domains.

If the Stabilize URLs for Visualforce, Experience Builder, Site.com Studio, and content files setting is enabled before you enable and deploy enhanced domains, these sandbox URL formats change.

URL TYPE	FORMAT	URL FORMAT
Content (Files)	Old	MyDomainName--SandboxName--c .documentforce.com
	New	MyDomainName--SandboxName .sandbox.file.force.com
Experience Builder	Old	MyDomainName--SandboxName .builder.salesforce-communities.com
	New	MyDomainName--SandboxName .sandbox.builder.salesforce-experience.com
Experience Builder Live Preview	Old	MyDomainName--SandboxName .livepreview.salesforce-communities.com
	New	MyDomainName--SandboxName .sandbox.live-preview.salesforce-experience.com
Experience Builder Preview	Old	MyDomainName--SandboxName .preview.salesforce-communities.com
	New	MyDomainName--SandboxName .sandbox.preview.salesforce-experience.com
Visualforce	Old	MyDomainName--SandboxName--PackageName .visualforce.com ¹
	New	MyDomainName--SandboxName--PackageName .sandbox.vf.force.com ¹

If the Stabilize URLs for Visualforce, Experience Builder, Site.com Studio, and content files setting isn't enabled before you enable and deploy enhanced domains, these sandbox URL formats change.

URL TYPE	FORMAT	URL FORMAT
Content (Files) in a non-Hyperforce org	Old	MyDomainName--SandboxName--c.InstanceName .content.force.com
	New	MyDomainName--SandboxName .sandbox.file.force.com

URL TYPE	FORMAT	URL FORMAT
Content (Files) in a Hyperforce org	Old	<i>MyDomainName-SandboxName-c.InstanceName</i> .content.sfdc- <i>HyperforceInstanceName</i> .force.com
	New	<i>MyDomainName--SandboxName</i> .sandbox.file.force.com
Experience Builder in a non-Hyperforce org	Old	<i>MyDomainName--SandboxName--sitestudio.InstanceName</i> .force.com
	New	<i>MyDomainName--SandboxName</i> .sandbox.builder.salesforce-experience.com
Experience Builder in a Hyperforce org	Old	<i>MyDomainName-SandboxName-sitestudio.InstanceName</i> .sfdc- <i>HyperforceInstanceName</i> .force.com
	New	<i>MyDomainName--SandboxName</i> .sandbox.builder.salesforce-experience.com
Experience Builder Live Preview in a non-Hyperforce org	Old	<i>MyDomainName--SandboxName--livepreview.InstanceName</i> .force.com
	New	<i>MyDomainName--SandboxName</i> .sandbox.live-preview.salesforce-experience.com
Experience Builder Live Preview in a Hyperforce org	Old	<i>MyDomainName-SandboxName-livepreview.InstanceName</i> .sfdc- <i>HyperforceInstanceName</i> .force.com
	New	<i>MyDomainName--SandboxName</i> .sandbox.live-preview.salesforce-experience.com
Experience Builder Preview in a non-Hyperforce org	Old	<i>MyDomainName--SandboxName--sitepreview.InstanceName</i> .force.com
	New	<i>MyDomainName--SandboxName</i> .sandbox.preview.salesforce-experience.com
Experience Builder Preview in a Hyperforce org	Old	<i>MyDomainName-SandboxName-sitepreview.InstanceName</i> .sfdc- <i>HyperforceInstanceName</i> .force.com
	New	<i>MyDomainName--SandboxName</i> .sandbox.preview.salesforce-experience.com
Visualforce in a non-Hyperforce org	Old	<i>MyDomainName--SandboxName--PackageName.InstanceName</i> .visual.force.com ¹
	New	<i>MyDomainName--SandboxName--PackageName</i> .sandbox.vf.force.com ¹
Visualforce in a Hyperforce org	Old	<i>MyDomainName-SandboxName-PackageName.InstanceName</i> .visual.sfdc- <i>HyperforceInstanceName</i> .force.com ¹
	New	<i>MyDomainName--SandboxName--PackageName</i> .sandbox.vf.force.com ¹

¹ If your installed package is unmanaged, the package name is *c*.

Changes to Instanced URLs Without My Domain

If your org was created before October 2020, you didn't get a My Domain by default. In that case, your users accessed Salesforce with these URLs that contained your instance name or a region identifier but not your My Domain name.

URL TYPE	FORMAT	URL FORMAT
Content (Files)	Old	<i>c.InstanceName</i> .content.force.com
	New in production	<i>MyDomainName</i> .file.force.com
	New in sandbox	<i>MyDomainName--SandboxName</i> .sandbox.file.force.com
Experience Builder (format 1)	Old	<i>ExperienceCloudSiteSubdomainName--builder.InstanceName</i> .force.com

URL TYPE	FORMAT	URL FORMAT
	New in production	MyDomainName .builder.salesforce-experience.com
	New in sandbox	MyDomainName--SandboxName .sandbox.builder.salesforce-experience.com
Experience Builder (format 2)	Old	sitestudio. InstanceName .force.com
	New in production	MyDomainName .builder.salesforce-experience.com
	New in sandbox	MyDomainName--SandboxName .sandbox.builder.salesforce-experience.com
Experience Builder Live Preview (format 1)	Old	ExperienceCloudSiteSubdomainName--live . InstanceName .force.com
	New in production	MyDomainName .live-preview.salesforce-experience.com
	New in sandbox	MyDomainName--SandboxName .sandbox.live-preview.salesforce-experience.com
Experience Builder Live Preview (format 2)	Old	livepreview. InstanceName .force.com
	New in production	MyDomainName .live-preview.salesforce-experience.com
	New in sandbox	MyDomainName--SandboxName .sandbox.live-preview.salesforce-experience.com
Experience Builder Preview (format 1)	Old	ExperienceCloudSiteSubdomainName--preview . InstanceName .force.com
	New in production	MyDomainName .preview.salesforce-experience.com
	New in sandbox	MyDomainName--SandboxName .sandbox.preview.salesforce-experience.com
Experience Builder Preview (format 2)	Old	sitepreview. InstanceName .force.com
	New in production	MyDomainName .preview.salesforce-experience.com
	New in sandbox	MyDomainName--SandboxName .sandbox.preview.salesforce-experience.com
Lightning page	Old	InstanceName .lightning.force.com
	New in production	MyDomainName .lightning.force.com
	New in sandbox	MyDomainName--SandboxName .sandbox.lightning.force.com
Next generation Omni-Channel engagement (examples: voice and messaging)	Old	Region .scrt.sfdc.sh
	New in production	MyDomainName .my.salesforce-scrt.com
	New in sandbox	MyDomainName--SandboxName .sandbox.my.salesforce-scrt.com
User Content	Old in production	InstanceName--UniqueID .a.forceusercontent.com
	New in production	MyDomainName--UniqueID .my.force-user-content.com
User Content in a sandbox	Old in sandbox	InstanceName--UniqueID .b.forceusercontent.com
	New in sandbox	MyDomainName--SandboxName--UniqueID .sandbox.my.force-user-content.com
User Content in a Government Cloud org	Old	InstanceName--UniqueID .c.forceusercontent.com
	New in production	MyDomainName--UniqueID .gia.force-user-content.com

URL TYPE	FORMAT	URL FORMAT
	New in sandbox	MyDomainName--SandboxName--UniqueID .sandbox.gia.force-user-content.com
Visualforce	Old	PackageName.InstanceName .visual.force.com ¹
	New in production	MyDomainName--PackageName .vf.force.com ¹
	New in sandbox	MyDomainName--SandboxName--PackageName .sandbox.vf.force.com ¹

¹ If your installed package is unmanaged, the package name is c.

SEE ALSO:

[My Domain](#)

[What Determines Your URL Formats](#)

[Update Your Org for My Domain Changes](#)

[Custom Domains](#)

Protect Your Salesforce Organization

Salesforce is built from the ground up to protect your data and applications. You can also implement your own security scheme to reflect the structure and needs of your organization. Protecting your data is a joint responsibility between you and Salesforce. The Salesforce security features enable you to empower your users to do their jobs safely and efficiently.

[Salesforce Security Basics](#)

The Salesforce security features help you empower your users to do their jobs safely and efficiently. Salesforce limits exposure of data to the users that act on it. Implement security controls that you think are appropriate for the sensitivity of your data. We'll work together to protect your data from unauthorized access from outside your company and from inappropriate usage by your users.

[Take Charge of Your Security Goals with Security Center](#)

The Security Center app offers a single view of your security, privacy, and governance posture across all of your Salesforce orgs and tenants. Use the app to review up-to-date health check scores, access settings, and user and login metrics in one easy-to-read interface. When you know how your orgs and tenants are performing, you can shorten security review processes and limit risks. You can also get clear insights into how you're meeting your security goals and respond proactively when suspicious conditions arise. And during periods of growth or change, Security Center can help you monitor changes that touch sensitive customer data.

[Einstein Data Detect](#)

Einstein Data Detect helps you identify sensitive data within your org so you can take steps to protect it. It uses native platform-native technology so that you don't rely on third-party services or port your data outside of Salesforce. Use Einstein Data Detect to expedite data categorization by aligning data sensitivity levels and categories to actual field data.

[Strengthen Your Data's Security with Shield Platform Encryption](#)

Shield Platform Encryption gives your data a whole new layer of security while preserving critical platform functionality. You can encrypt sensitive data at rest, and not just when transmitted over a network, so your company can confidently comply with privacy policies, regulatory requirements, and contractual obligations for handling private data.

[Limit Interactions with External URLs and Origins](#)

In our connected world, interaction with external websites and origins is a necessity. To protect your network and data, configure allowlists and enable settings that limit how Salesforce and external origins interact. And limit redirections that originate in Salesforce to URLs that you trust.

[Configure Clickjack Protection](#)

Clickjacking is a type of attack that tricks users into clicking something, such as a button or link. The click sends an HTTP request that performs malicious actions that can lead to data intrusion, unauthorized emails, changed credentials, or similar results. To help protect against this kind of attack, most Salesforce pages can only be served in an inline frame by a page on the same domain. Learn which types of pages can be framed and how to configure the related clickjack settings.

[Session Security](#)

After logging in, a user establishes a session with the platform. Use session security to limit exposure to your network when a user leaves the computer unattended while still logged in. Session security also limits the risk of internal attacks, such as when one employee tries to use another employee's session. Choose from several session settings to control session behavior.

[Secure Cross-Cloud Integrations with Private Connect](#)

When you integrate your Salesforce org with applications hosted on third-party cloud services, it's essential to be able to send and receive HTTP/s traffic securely. With Private Connect, increase security on your Amazon Web Services (AWS) integrations by setting up a fully managed network connection between your Salesforce org and your AWS Virtual Private Cloud (VPC). Then, route your cross-cloud traffic through the connection instead of over the public internet to reduce exposure to outsider security threats.

[Activations](#)

Activation tracks information about devices from which users have verified their identity. Salesforce prompts users to verify their identity when they access Salesforce from an unrecognized browser or application. Identity verification adds an extra layer of security on top of username and password authentication. The Activations page lists the login IP addresses and client browsers used.

[Real-Time Event Monitoring](#)

Real-Time Event Monitoring helps you monitor and detect standard events in Salesforce in near real-time. You can store the event data for auditing or reporting purposes. You can create transaction security policies using Condition Builder—a point-and-click tool—or Apex code.

[Configure Remote Site Settings](#)

Configure settings for a remote site.

[Named Credentials](#)

A named credential specifies the URL of a callout endpoint and its required authentication parameters in one definition. To simplify the setup of authenticated callouts, specify a named credential as the callout endpoint.

[Certificates and Keys](#)

Salesforce certificates and key pairs are used for signatures that verify a request is coming from your organization. They are used for authenticated SSL communications with an external website, or when using your organization as an Identity Provider. You only need to generate a Salesforce certificate and key pair if you're working with an external website that wants verification that a request is coming from a Salesforce organization.

Salesforce Security Basics

The Salesforce security features help you empower your users to do their jobs safely and efficiently. Salesforce limits exposure of data to the users that act on it. Implement security controls that you think are appropriate for the sensitivity of your data. We'll work together to protect your data from unauthorized access from outside your company and from inappropriate usage by your users.

Phishing and Malware

If you see something suspicious related to your Salesforce implementation, report it to security@salesforce.com, in addition to your own IT or security team. Trust starts with transparency. That's why Salesforce displays real-time information on system performance and security at <https://trust.salesforce.com>. For security-specific information, go to <https://trust.salesforce.com/security>. This site provides live data on system performance, alerts for current and recent phishing and malware attempts, and tips on security best practices for your organization.

Security Infrastructure

Salesforce utilizes some of the most advanced technology for Internet security available today. When you access the application using a Salesforce-supported browser, Transport Layer Security (TLS) technology protects your information using both server authentication and Classic Encryption, ensuring that your data is safe, secure, and available only to registered users in your organization.

Security Health Check

As an admin, you can use Health Check to identify and fix potential vulnerabilities in your security settings, all from a single page. A summary score shows how your org measures against a security baseline like the Salesforce Baseline Standard. You can upload up to five custom baselines to use instead of the Salesforce Baseline Standard.

Auditing

Auditing provides information about use of the system, which can be critical in diagnosing potential or real security issues. Salesforce auditing features don't secure your organization by themselves. Have someone in your organization perform regular audits to detect potential abuse.

Salesforce Shield

Salesforce Shield is a trio of security tools that helps you build extra levels of trust, compliance, and governance right into your business-critical apps. It includes Shield Platform Encryption, Event Monitoring, and Field Audit Trail. Ask your Salesforce administrator if Salesforce Shield is available in your org.

SEE ALSO:

[Security Implementation Guide](#)

Phishing and Malware

If you see something suspicious related to your Salesforce implementation, report it to security@salesforce.com, in addition to your own IT or security team. Trust starts with transparency. That's why Salesforce displays real-time information on system performance and security at <https://trust.salesforce.com>. For security-specific information, go to <https://trust.salesforce.com/security>. This site provides live data on system performance, alerts for current and recent phishing and malware attempts, and tips on security best practices for your organization.

The Security section of the Trust site includes valuable information that can help you safeguard your company's data. In addition to security best practices, the site provides information on how to recognize and report phishing attempts and information on current malware campaigns that could impact Salesforce customers.

- Phishing is a social engineering technique that attempts to acquire sensitive information, such as usernames, passwords, and credit card details, by masquerading as a trustworthy person or entity. Phishing can occur via email, text messaging, voice calls, and other avenues. Phishers often direct targets to click a link and enter valuable information or to open an attachment with the goal of downloading malware onto the target's device. As the Salesforce community grows, it becomes an increasingly appealing target for phishers. You'll never get an email or a phone call from a Salesforce employee asking you to reveal your login credentials, so don't reveal them to anyone. Report suspicious activities or emails regarding your Salesforce instance directly to the Salesforce Security team at security@salesforce.com.
- Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. It's a general term used to cover various forms of hostile or intrusive software, including computer viruses and spyware. For a list of current security advisories, go to <https://trust.salesforce.com/en/security/security-advisories>.

What Salesforce Is Doing About Phishing and Malware

Security is the foundation of our customers' success, so Salesforce continues to implement the best possible practices and security technologies to protect our ecosystem. Recent and ongoing actions include:

- Actively monitoring and analyzing logs to enable alerts to our customers who have been affected.
- Collaborating with leading security vendors and experts on the most effective security tools.
- Ongoing security education and engagement activities for Salesforce employees.
- Creating processes for developing products with security in mind.
- Proactively sharing security best practices with customers and partners through trust.salesforce.com/security and other ongoing activities.

What Salesforce Recommends You Do

Salesforce is committed to setting the standards in software-as-a-service as an effective partner in customer security. In addition to our internal efforts, Salesforce strongly recommends that customers implement the following changes to enhance security.

- To safeguard access to your network, Salesforce requires that all logins use multi-factor authentication (MFA).
- To activate IP range restrictions, modify your Salesforce implementation. These restrictions allow users to access Salesforce only from your corporate network or VPN. For more information, see [Set Trusted IP Ranges for Your Organization](#).
- Set session security restrictions to make spoofing more difficult. For more information, see [Modify Session Security Settings](#).
- Educate your employees not to open suspect emails and to be vigilant in guarding against phishing attempts.
- Use security solutions from leading vendors to deploy spam filtering and malware protection.
- Designate a security contact within your organization so that Salesforce can more effectively communicate with you. Contact your Salesforce representative with this information.
- Use Enhanced Transaction Security to monitor events and take appropriate actions. For more information, see [Enhanced Transaction Security](#).

Salesforce has a Security Incident Response Team to respond to any security issues. To report a security incident or vulnerability to Salesforce, contact security@salesforce.com. Describe the issue in detail, and the team will respond promptly.

Email Awareness Best Practices

Phishing scams use fraudulent emails to get users to reveal confidential information. Such emails typically look like they come from a legitimate organization and can contain links to what appears to be that organization's site. However, the site is actually a fake site designed to capture information.

As these scams get more sophisticated, it can be tough to know whether an email is real or fake. For example, phishing emails can include malicious links from `force.com` domains. And Salesforce orgs that generate cases from inbound email can include malicious content from those emails in the cases themselves.

The best way to avoid becoming the victim of a phishing or malware attack is to know what to look for. We recommend that you apply the same best practices for cases generated through Salesforce as you do for phishing emails:

- Don't click links or open attachments in emails and email-generated cases, unless you were expecting to receive it.
- Treat all emails and cases originating from external email addresses as potentially untrustworthy.
- If an email or email-generated case contains messages instructing you to do any of the following, it's most likely a phishing attempt:
 - Click a link.
 - Open an attachment.
 - Validate your password.

- Log in to your account.
- Enter personal details or credentials.

If you receive a phishing email or Email-to-Case, delete it and notify your internal IT team. We appreciate your trust in us as we continue to make your success our top priority.

Security Infrastructure

Salesforce utilizes some of the most advanced technology for Internet security available today. When you access the application using a Salesforce-supported browser, Transport Layer Security (TLS) technology protects your information using both server authentication and Classic Encryption, ensuring that your data is safe, secure, and available only to registered users in your organization.

One of the core features of a multi-tenant platform is the use of a single pool of computing resources to service the needs of many different customers. Salesforce protects your organization's data from all other customer organizations by using a unique organization identifier, which is associated with each user's session. Once you log in to your organization, your subsequent requests are associated with your organization, using this identifier.

In addition, Salesforce is hosted in a secure server environment that uses a firewall and other advanced technology to prevent interference or access from outside intruders.

Salesforce requires that cipher suites used for outbound calls meet security standards. Check your servers' cipher suite lists and ensure that they support the advanced encryption standard (AES) with 128-bit (AES128) or 256-bit (AES256) stream keys. Otherwise, custom code that relies on outbound calls to the HTTPS server fails.

SEE ALSO:

[Knowledge Article: Salesforce Services and Marketing Cloud supported Cipher Suites for outbound calls](#)

Security Health Check

As an admin, you can use Health Check to identify and fix potential vulnerabilities in your security settings, all from a single page. A summary score shows how your org measures against a security baseline like the Salesforce Baseline Standard. You can upload up to five custom baselines to use instead of the Salesforce Baseline Standard.

From Setup, in the Quick Find box, enter *Health Check*, and then select **Health Check**.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To view Health Check and export custom baselines:

- View Health Check
- OR
- View Security Center
- Or
- Manage Security Center

To import custom baselines:

- Manage Health Check
- OR
- View Security Center
- Or
- Manage Security Center

STATUS	SETTING	GROUP	YOUR VALUE	STANDARD VALUE	ACTIONS
Critical	Enable clickjack protection for customer Visualforce pages with standard headers	Session Settings	Disabled	Enabled	Edit

In the baseline dropdown (1), choose the Salesforce Baseline Standard or a custom baseline. The baseline consists of recommended values for High-Risk, Medium-Risk, Low-Risk, and Informational Security Settings (2). If you change settings to be less restrictive than in the baseline, your health check score (3) and grade (4) decreases.

Your settings are shown with information about how they compare against baseline values (5). To remediate a risk, edit the setting (6) or use Fix Risks (7) to quickly change settings to your selected baseline's recommended values without leaving the Health Check page. You can import, export, edit, or delete a custom baseline with the baseline control menu (8).

 **Note:** New settings to Security Health Check are added to the Salesforce Baseline Standard with default values. If you have a custom baseline, you're prompted to add the new settings when you open it.

 **Example:** Suppose that you changed your password minimum length from 8 (the default value) to 5, and changed other Password Policies settings to be less restrictive. These changes make your users' passwords more vulnerable to guessing and other brute force attacks. As a result, your overall score decreases and the settings are listed as risks.

Fix Risks Limitations

Not all settings can be changed using the Fix Risks button. If a setting you want to adjust doesn't appear on the Fix Risks screen, change it manually using the Edit link on the Health Check page. The Health Check detail page in the Security Center app saves you time by aggregating multiple Health Check scores and settings in one place. For more information, see [Take Charge of Your Security Goals with Security Center](#) on page 896.

[How Is the Health Check Score Calculated?](#)

The Health Check score is calculated by a proprietary formula that measures how well your security settings meet either the Salesforce Baseline Standard or your selected custom baseline. Settings that meet or exceed compliance raise your score, and settings at risk lower your score.

[Create a Custom Baseline for Health Check](#)

You can import up to five custom baselines to compare your security settings with your standards instead of the Salesforce recommended standards. For example, if you're in financial services, you can create a custom security baseline by using FINRA standards.

[Custom Baseline File Requirements](#)

To import your Health Check custom baseline successfully, make sure that your file and settings meet the requirements.

SEE ALSO:

[How Is the Health Check Score Calculated?](#)

[Review Health Check Data](#)

[Security Implementation Guide](#)

How Is the Health Check Score Calculated?

The Health Check score is calculated by a proprietary formula that measures how well your security settings meet either the Salesforce Baseline Standard or your selected custom baseline. Settings that meet or exceed compliance raise your score, and settings at risk lower your score.

There are four risk categories: High-Risk, Medium-Risk, Low-Risk, and Informational. The risk categories affect your Health Check score, with High-Risk settings counting the most, Low-Risk settings counting the least, and Medium-Risk settings in the middle. Settings in the Informational category don't factor in to your Health Check score.

If all settings meet or exceed the standard, your total score is 100%. As you update your settings, your green bar moves to the right.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions



Your grade is based on your score.

- 90% and above = Excellent
- 80%–89% = Very Good
- 70%–79% = Good
- 55%–69% = Poor
- 54% and below = Very Poor

 **Note:** Here are important considerations about your Health Check score.

- You can see your score on the Health Check page but not through the API.
- Your score can change if Salesforce adds or removes options that are used in the score calculation.

Recommended Actions Based on Your Score

If your total score is...	We recommend that you...
0%–33%	Remediate high risks immediately.
34%–66%	Remediate high risks in the short term and medium risks in the long term.
67%–100%	Review Health Check periodically to remediate risks.

 **Note:** New Salesforce orgs have an initial score less than 100%. Use Health Check to quickly improve your score by eliminating high risks in your Password Policies and other setting groups.

These are the Salesforce baseline standard settings, risk levels, and values from the default Salesforce Baseline Standard. If you're using a custom baseline, your information differs.

High Risk Security Settings

Setting	Compliant Value	Warning Value	Critical Value
Lock sessions to the domain in which they were first used	Checkbox selected	N/A	Checkbox deselected
Enable the SMS method of device activation	Checkbox selected	N/A	Checkbox deselected
Enable clickjack protection for Setup pages	Checkbox selected	N/A	Checkbox deselected
Enable clickjack protection for non-Setup for Salesforce pages	Checkbox selected	N/A	Checkbox deselected
Enable clickjack protection for customer VisualForce pages with standard headers	Checkbox selected	N/A	Checkbox deselected
Enable clickjack protection for customer VisualForce pages with headers disabled	Checkbox selected	N/A	Checkbox deselected

Setting	Compliant Value	Warning Value	Critical Value
Enable CSRF protection on GET requests on non-setup pages	Checkbox selected	N/A	Checkbox deselected
Enable CSRF protection on POST requests on non-setup pages	Checkbox selected	N/A	Checkbox deselected
Require HttpOnly attribute	Checkbox selected	Checkbox deselected	N/A
Number of security risk file types with hybrid behavior	No security risk file types have hybrid behavior enabled	One or more security risk file types has hybrid behavior enabled	N/A
Maximum invalid login attempts	3	5, 10	No Limit
Number of expired certificates	No certificates have expired	One or more certificates have expired	N/A
Number of Objects with Default External Access Set to Public	No objects with default external access set to public exist	At least one object with default external access set to public exists	N/A

Medium Risk Security Settings

Setting	Compliant Value	Warning Value	Critical Value
Require a minimum 1 day password lifetime	Checkbox selected	Checkbox deselected	N/A
Force relogin after Login-As-User	Checkbox selected	N/A	Checkbox deselected
Enforce login IP ranges on every request	Checkbox selected	Checkbox deselected	N/A
Enable Content Security Policy protection for email templates	Checkbox selected	N/A	Checkbox deselected
Enable Content Sniffing protection	Checkbox selected	N/A	Checkbox deselected
Administrators Can Log In As Any User	Checkbox deselected	Checkbox selected	N/A
Enforce password history	3 or more passwords remembered	1 or 2 passwords remembered	No passwords remembered
Minimum password length	8	6 or 7	5 or less
User passwords expire in	90 days or less	180 days	One year or Never expires
Password complexity requirement	Must mix alpha, numeric, and special characters, or more complex	Must mix alpha and numeric characters	No restriction

Low Risk Security Settings

Setting	Compliant Value	Warning Value	Critical Value
Obscure secret answer for password resets	Checkbox selected	Checkbox deselected	N/A
Force logout on session timeout	Checkbox selected	Checkbox deselected	N/A
Require identity verification during multi-factor authentication (MFA) registration	Checkbox selected	N/A	Checkbox deselected
Require identity verification for change of email address	Checkbox selected	N/A	Checkbox deselected
Remote Site	No remote sites with the Disable Protocol Security option selected	At least one remote site created with the Disable Protocol Security option selected.	N/A
Password question requirement	Can't contain password	None	N/A
Timeout Value	2 hours or less	4, 8, or 12 hours	Checkbox deselected
Lockout effective period	30 minutes or greater	Less than 30 minutes	N/A

Informational Security Settings

Informational Security settings don't affect your Health Check score, but are valuable to review.

Setting	Compliant Value	Warning Value	Critical Value
Allow redirections to untrusted external URLs without warning	Setting is disabled	N/A	Setting is enabled
Days until certificate expiration	No certificates created, or all certificates have more than 180 days until expiration	Less than 180 days but more than 15 days until expiration of at least one certificate	Less than 15 days until expiration of at least one certificate
Key Size	All certificates have a key size of 4096	At least one certificate has a key size of 2048	N/A
Number of Objects to which Guest User Profiles have Edit Access	0–4	5–9	10 or more
Number of Objects to which Guest User Profiles have Read Access	0–4	5–9	10 or more
Require permission to view record names in lookup fields	Setting is enabled	N/A	Setting is disabled

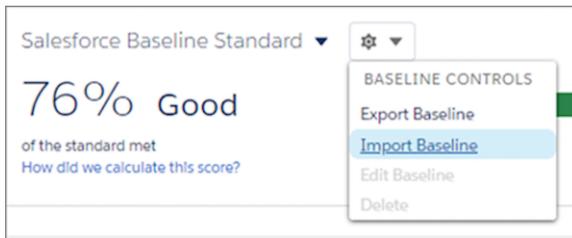
SEE ALSO:

[Security Health Check](#)

Create a Custom Baseline for Health Check

You can import up to five custom baselines to compare your security settings with your standards instead of the Salesforce recommended standards. For example, if you're in financial services, you can create a custom security baseline by using FINRA standards.

To create a custom baseline, start with the Salesforce Baseline Standard.



1. To export the Salesforce Baseline Standard file, from the Baseline Controls menu, select **Export Baseline**.
2. Edit the XML file with a text editor and save your changes.
 - a. Adjust the risk categories to customize your scoring. The risk category affects your Health Check score. A setting in a higher risk category is weighted as more important than a lower one. Moving a setting to the Informational category removes it from the Health Check score calculation.
 - b. To modify the setting values, follow the Custom Baseline File Requirements. You can't change some values, and some settings have restricted value options. Don't add or delete risk categories, setting names, or quotation marks. If you do, your import fails. In some security settings, a low value can be low risk, but in others, it can be high risk. For example, the lower your minimum password length value is, the riskier it is. But the lower your maximum invalid login attempts value is, the safer it is.
3. To import a file, from the Baselines Controls menu, select **Import Baseline**.
 - a. Name your custom baseline. Spaces and some special characters are allowed. If the name is SFDC recommended or Salesforce Baseline Standard, the file fails to import.
 - b. Give your custom baseline a unique API name. You can use letters and numbers, but the name must begin with a letter. It can't contain spaces or special characters.
 - c. Optionally, make your custom baseline the default baseline in Security Health Check.

Unexpected information in the baseline file or a new custom baseline upload without all Health Check settings results in an import failure. If your import fails, you receive a message to help resolve the problem. See Custom Baseline File Requirements in Salesforce Help for troubleshooting assistance. You can change the baseline name, API name, and default baseline using the Edit feature in the Baseline Controls menu.
4. To confirm that your file uploaded, click the baseline dropdown and select your baseline. If you set your custom baseline as the default, it appears after import.

EDITIONS

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To view a custom baseline

- View Health Check

OR

View Security Center

OR

Manage Security Center

To create a custom baseline

- Manage Health Check

OR

View Security Center

Or

Manage Security Center



SEE ALSO:

- [Custom Baseline File Requirements](#)
- [How Is the Health Check Score Calculated?](#)
- [Security Health Check](#)

Custom Baseline File Requirements

To import your Health Check custom baseline successfully, make sure that your file and settings meet the requirements.

XML File

Use a valid XML file with only English language characters. The file can't be larger than 20 KB. Make sure that each value is surrounded in quotation marks.

EDITIONS

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer Editions**

Custom Baseline Security Setting Fields and Values

You can't add or delete the Health Check settings from the file, but you can change their risks and values.

There are four risk categories: High-Risk, Medium-Risk, Low-Risk, and Informational. The risk categories affect your Health Check score, with High-Risk settings counting the most, Low-Risk settings counting the least, and Medium-Risk settings in the middle. You can move settings into any risk category. Settings in the Informational category don't factor into your Health Check score, so move unnecessary settings to this category rather than deleting them.

Each security setting shows in Health Check as compliant, warning, or critical. These statuses guide you to increase security. Assign values to each status in the import file.

There are three setting types: boolean, numeric range, and enum. The values you can assign to each setting depend on the setting type.

Boolean Security Settings

Boolean settings have two attributes: compliant and noncompliant. Compliant values correspond to checkboxes in security settings. A Boolean value of `"true"` indicates selecting the checkbox, and `"false"` represents deselecting it. Noncompliant attributes can take either `warning` or `critical` values.

 **Important:** You can't change boolean compliant values in Health Check, but you can change noncompliant values.

Setting	Accepted Values
LoginAccessPolicies.adminLoginAsAnyUser	<ul style="list-style-type: none"> • <code>"false"</code>—compliant • <code>"warning"</code> or <code>"critical"</code>—noncompliant
PasswordPolicies.minOneDayPasswordLifetime	<ul style="list-style-type: none"> • <code>"true"</code>—compliant • <code>"warning"</code> or <code>"critical"</code>—noncompliant
PasswordPolicies.obscureSecretAnswer	<ul style="list-style-type: none"> • <code>"true"</code>—compliant • <code>"warning"</code> or <code>"critical"</code>—noncompliant

Setting	Accepted Values
SessionSettings.clickjackNonSetup	<ul style="list-style-type: none"> • "true"—compliant • "warning" or "critical"—noncompliant
SessionSettings.clickjackSetup	<ul style="list-style-type: none"> • "true"—compliant • "warning" or "critical"—noncompliant
SessionSettings.clickjackVisualForceHeaders	<ul style="list-style-type: none"> • "true"—compliant • "warning" or "critical"—noncompliant
SessionSettings.clickjackVisualForceNoHeaders	<ul style="list-style-type: none"> • "true"—compliant • "warning" or "critical"—noncompliant
SessionSettings.contentSniffingProtection	<ul style="list-style-type: none"> • "true"—compliant • "warning" or "critical"—noncompliant
SessionSettings.cspOnEmail	<ul style="list-style-type: none"> • "true"—compliant • "warning" or "critical"—noncompliant
SessionSettings.csrfGet	<ul style="list-style-type: none"> • "true"—compliant • "warning" or "critical"—noncompliant
SessionSettings.csrfPost	<ul style="list-style-type: none"> • "true"—compliant • "warning" or "critical"—noncompliant
SessionSettings.enableSmsIdentity	<ul style="list-style-type: none"> • "true"—compliant • "warning" or "critical"—noncompliant
SessionSettings.enforceLoginIp	<ul style="list-style-type: none"> • "true"—compliant • "warning" or "critical"—noncompliant
SessionSettings.forceLogoutOnTimeout	<ul style="list-style-type: none"> • "true"—compliant • "warning" or "critical"—noncompliant
SessionSettings.forceRelogin	<ul style="list-style-type: none"> • "true"—compliant • "warning" or "critical"—noncompliant
SessionSettings.icOn2faRegistration	<ul style="list-style-type: none"> • "true"—compliant • "warning" or "critical"—noncompliant
SessionSettings.icOnEmailChange	<ul style="list-style-type: none"> • "true"—compliant

Setting	Accepted Values
	<ul style="list-style-type: none"> • “warning” or “critical”—noncompliant
SessionSettings.lockSessionsToDomain	<ul style="list-style-type: none"> • “true”—compliant • “warning” or “critical”—noncompliant
SessionSettings.redirectionAllowUntrusted	<ul style="list-style-type: none"> • “true”—noncompliant • “warning” or “critical”—compliant
SessionSettings.requireHttpOnly	<ul style="list-style-type: none"> • “true”— compliant • “warning” or “critical”— noncompliant
SessionSettings.xssProtection	<ul style="list-style-type: none"> • “true”— compliant • “warning” or “critical”— noncompliant
UserPIISettings.enforceNameVisibility	<ul style="list-style-type: none"> • “enabled”— compliant • “disabled”— noncompliant

Numeric Range Security Settings

Numeric range values are positive integers extended to one decimal place. You provide compliant and warning values only for numeric range settings. Critical values are assumed based on the other values in the settings. Each setting has specific validation rules, so enter only acceptable values.

Setting	Compliant Value	Warning Value
CertificateAndKeyManagement.certExpiration	Number of days—any integer between “0.0” and “180.0”	Any integer between “0.0” and “180.0” that is less than the compliant value. Any value less than the warning value shows as critical.
CertificateAndKeyManagement.expiredCert	Any integer “0.0” or greater	Any integer greater than the compliant value. Any value greater than the warning value shows as critical.
CertificateAndKeyManagement.keySize	“4096.0” or “2048.0”	“4096.0” or “2048.0.” To not allow the 2048 key size, enter a compliant value of “4096.0” and a warning value of any number between “2048.0” and “4096.0.”
FileUploadAndDownloadSecurity.hybridSecurityRiskFileTypes	Any integer “0.0” or greater	Any integer greater than the compliant value. Any value greater than the warning value shows as critical.
GuestUserAccess.guestEditAccess	Any integer “0.0” through “4.0”	Any integer “5.0” through “9.0”. Any value “10.0” or greater shows as critical.
GuestUserAccess.guestReadAccess	Any integer “0.0” through “4.0”	Any integer “5.0” through “9.0”. Any value “10.0” or greater shows as critical.

Setting	Compliant Value	Warning Value
PasswordPolicies.history	Any integer between "0.0" and "24.0"	Any integer between "0.0" and "24.0" that is less than the compliant value. Any value less than the warning value shows as critical.
PasswordPolicies.minPasswordLength	Any integer between "5.0" and "50.0"	Any integer between "5.0" and "50.0" that is less than the compliant value. Any value less than the warning value shows as critical.
RemoteSiteSettings.remoteSiteSettings	Maximum number of remote site settings allowed—any integer greater than "0.0"	Any integer greater than the compliant value. Any value greater than the warning value shows as critical.
SharingSettings.orgWideDefaults	Any integer between "0.0" and "1.0"	Any integer between "0.0" and "1.0" that is greater than the compliant value.

Enum Security Settings

Enum values allow you to choose from provided string texts. Use all the possible values, and decide whether they're compliant, warning, or critical status. Enum values are case sensitive. You can assign multiple enum names to one status by separating them with commas. For example, `compliant="FifteenMinutes,ThirtyMinutes,SixtyMinutes,TwoHours"`.

To leave a status empty, use all values. For example, divide the values between compliant and critical and leave warning empty: `warning=""`. Don't leave the compliant status empty.

 **Important:** Use every accepted value in each setting. If a value is missing, the file doesn't import.

Setting	Accepted Values
PasswordPolicies.complexity	<ul style="list-style-type: none"> • "UpperLowerCaseNumericSpecialCharacters" • "UpperLowerCaseNumeric" • "SpecialCharacters" • "AlphaNumeric" • "NoRestriction" (highest risk)
PasswordPolicies.expiration	<ul style="list-style-type: none"> • "ThirtyDays" • "SixtyDays" • "NinetyDays" • "SixMonths" • "OneYear" • "Never" (highest risk)
PasswordPolicies.lockoutInterval	<ul style="list-style-type: none"> • "Forever" (admin must reset) • "SixtyMinutes" • "ThirtyMinutes" • "FifteenMinutes" (highest risk)

Setting	Accepted Values
PasswordPolicies.maxLoginAttempts	<ul style="list-style-type: none">• "ThreeAttempts"• "FiveAttempts"• "TenAttempts"• "NoLimit" (highest risk)
PasswordPolicies.questionRestriction	<ul style="list-style-type: none">• "DoesNotContainPassword"• "None" (highest risk)
SessionSettings.timeout	<ul style="list-style-type: none">• "FifteenMinutes"• "ThirtyMinutes"• "SixtyMinutes"• "TwoHours"• "FourHours"• "EightHours"• "TwelveHours"• "TwentyFourHours" (highest risk)

 Example:

```

<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<!-- Please read Custom Baseline File Requirements for information about making changes in this file:
https://help.salesforce.com/articleView?id=security_custom_baseline_file_requirements.htm -->
<baseline xsi:noNamespaceSchemaLocation="security-risk-baseline.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" developerName="SFDCRecommended" name="SFDC recommended">
  - <highRiskSecuritySettings>
    <booleanSetting name="SessionSettings.lockSessionsToDomain" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.enableSmsIdentity" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.clickjackSetup" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.clickjackNonSetup" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.clickjackVisualForceHeaders" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.clickjackVisualForceNoHeaders" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.csrfGet" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.csrfPost" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.requireSecureConnections" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.requireHttpOnly" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.upgradeInsecureRequests" nonCompliant="critical" compliant="true"/>
    <numericRangeSetting name="FileUploadAndDownloadSecurity.hybridSecurityRiskFileTypes" compliant="0.0"
      warning="0.5"/>
    <enumSetting name="PasswordPolicies.maxLoginAttempts" compliant="ThreeAttempts"
      warning="FiveAttempts,TenAttempts" critical="NoLimit"/>
    <numericRangeSetting name="CertificateAndKeyManagement.expiredCert" compliant="0.0" warning="1.0"/>
  </highRiskSecuritySettings>
  - <mediumRiskSecuritySettings>
    <booleanSetting name="PasswordPolicies.minOneDayPasswordLifetime" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.forceReLogin" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.enforceLoginIp" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.cspOnEmail" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.xssProtection" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.contentSniffingProtection" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="LoginAccessPolicies.adminLoginAsAnyUser" nonCompliant="critical" compliant="false"/>
    <numericRangeSetting name="PasswordPolicies.history" compliant="3.0" warning="1.0"/>
    <numericRangeSetting name="PasswordPolicies.minPasswordLength" compliant="8.0" warning="6.0"/>
    <enumSetting name="PasswordPolicies.expiration" compliant="ThirtyDays,SixtyDays,NinetyDays"
      warning="SixMonths" critical="OneYear,Never"/>
    <enumSetting name="PasswordPolicies.complexity"
      compliant="SpecialCharacters,UpperLowerCaseNumeric,UpperLowerCaseNumericSpecialCharacters"
      warning="AlphaNumeric" critical="NoRestriction"/>
  </mediumRiskSecuritySettings>
  - <lowRiskSecuritySettings>
    <booleanSetting name="PasswordPolicies.obscureSecretAnswer" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.forceLogoutOnTimeout" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.icOn2faRegistration" nonCompliant="critical" compliant="true"/>
    <booleanSetting name="SessionSettings.icOnEmailChange" nonCompliant="critical" compliant="true"/>
    <numericRangeSetting name="RemoteSiteSettings.remoteSiteSettings" compliant="0.0" warning="1.0"/>
    <enumSetting name="PasswordPolicies.questionRestriction" compliant="DoesNotContainPassword" warning="None"/>
    <enumSetting name="PasswordPolicies.lockoutInterval" compliant="ThirtyMinutes,SixtyMinutes,Forever"
      warning="FifteenMinutes"/>
    <enumSetting name="SessionSettings.timeout" compliant="FifteenMinutes,ThirtyMinutes,SixtyMinutes,TwoHours"
      warning="FourHours,EightHours,TwelveHours" critical="TwentyFourHours"/>
  </lowRiskSecuritySettings>
  - <informationalSecuritySettings>
    <numericRangeSetting name="CertificateAndKeyManagement.keySize" compliant="4096.0" warning="2048.0"/>
    <numericRangeSetting name="CertificateAndKeyManagement.certExpiration" compliant="180.0" warning="1.0"/>
    <booleanSetting name="SessionSettings.hstsOnForcecomSites" nonCompliant="critical" compliant="true"/>
  </informationalSecuritySettings>
</baseline>

```

SEE ALSO:

[Create a Custom Baseline for Health Check](#)

Auditing

Auditing provides information about use of the system, which can be critical in diagnosing potential or real security issues. Salesforce auditing features don't secure your organization by themselves. Have someone in your organization perform regular audits to detect potential abuse.

To verify that your system is secure, monitor for unexpected changes or usage trends.

Record Modification Fields

All objects include fields to store the name of the user who created the record and who last modified the record. These fields provide basic auditing information.

Login History

You can review a list of successful and failed login attempts to your organization for the past 6 months.

Field History Tracking

You can enable auditing for individual fields, which automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.

Setup Audit Trail

Administrators can view a Setup Audit Trail, which logs when modifications are made to your organization's configuration.

Salesforce Shield

Salesforce Shield is a trio of security tools that helps you build extra levels of trust, compliance, and governance right into your business-critical apps. It includes Shield Platform Encryption, Event Monitoring, and Field Audit Trail. Ask your Salesforce administrator if Salesforce Shield is available in your org.

Shield Platform Encryption

Shield Platform Encryption allows you to natively encrypt your most sensitive data at rest across all your Salesforce apps. Encrypting data at rest adds another layer of protection to PII, sensitive, confidential, or proprietary data. It also helps you meet external and internal data compliance policies while keeping critical app functionality such as search, workflow, and validation rules. You keep full control over encryption keys and can set encrypted data permissions to protect sensitive data from unauthorized users. See [Shield Platform Encryption](#) on page 920

Real-Time Event Monitoring

Real-Time Event Monitoring gives you access to detailed performance, security, and usage data on all your Salesforce apps. See who is accessing critical business data when, and from where. Understand user adoption across your apps. Troubleshoot and optimize performance to improve the end-user experience. Event Monitoring data is tracked via the API and can be imported into any data visualization or application monitoring tool, like Analytics, Splunk, or New Relic. To get started, check out our [Event Monitoring](#) training course.

Field Audit Trail

With Field Audit Trail, you know the state and value of your data for any date at any time. You can use it for regulatory compliance, internal governance, audit, or customer service. Field Audit trail is built on a big data backend for massive scalability, and you can use it to create a forensic data-level audit trail. See [Field Audit Trail](#) on page 1244.

Einstein Data Detect

With Einstein Data Detect you can scan your org for sensitive data and then take steps to protect it. You expedite data categorization by aligning data sensitivity levels and categories to actual field data. And you no longer rely on third-party services or port your data outside of Salesforce. See [Einstein Data Detect](#) on page 914.

Shield Learning Map: Find Learning Resources and Documentation

The Shield Learning Map is a friendly, centralized resource for all things Shield. No matter which Shield product you buy or how you plan to use it, the learning map offers a clear path toward success. You can find links to the Shield Learning Map from Shield product documentation, or go directly to <https://shieldlearningmap.com>.

On the landing page, get oriented to Shield with Dreamforce presentations, videos, and overview documentation. Then click the trail to see resources—developer guides, how-to steps, Trailhead, and best practices—targeted at specific features and use cases. From planning security policies to putting those policies into action, the map offers you just-in-time information for all stages of your Shield journey.



And if you want to ask questions or find the latest information about Shield improvements, the map has you covered. The button bar at the bottom of the map offers links to Shield-specific Trailblazer Community groups, discussion forums, on-demand webinars, and release notes.

Take Charge of Your Security Goals with Security Center

The Security Center app offers a single view of your security, privacy, and governance posture across all of your Salesforce orgs and tenants. Use the app to review up-to-date health check scores, access settings, and user and login metrics in one easy-to-read interface. When you know how your orgs and tenants are performing, you can shorten security review processes and limit risks. You can also get clear insights into how you're meeting your security goals and respond proactively when suspicious conditions arise. And during periods of growth or change, Security Center can help you monitor changes that touch sensitive customer data.

Available in: **Enterprise, Performance, Unlimited**, and **Developer** Editions. Requires the Security Center add-on subscription.

Available in: Lightning Experience

[Security Center Definitions](#)

Keep these terms in mind when working with Security Center.

[Enable Security Center Permissions](#)

To give new users access to Security Center in the app launcher, enable Security Center permissions. You can assign Security Center permissions from Profiles or Permission Sets in Setup.

[Designate a Parent Tenant in Security Center](#)

To see security information for multiple tenants, designate a parent tenant to show data collected from that parent tenant and all connected child tenants. You can disconnect child tenants at any time. And you can group parent and child tenants based on their security policies or regulations.

[Security Center Data](#)

Security Center offers several ways to view your security settings and data. Summary and Category dashboards organize aggregate data and totals for quick scanning. Detail pages show metric-specific trends and details about changes made to security settings on specific days. Security Center stores data for 6 months. Because Security Center surfaces sensitive information, we recommend that you enable multi-factor authentication for all Security Center users.

[Create Alerts for Security Changes](#)

Create custom alerts to immediately learn about changes made to security settings that you care about. Alerts notify you by email or in the Salesforce app when a setting in your Security Center tenant exceeds a threshold that you set. Create as many alerts as you want so that you can stay informed of your tenant's security posture.

[Define and Deploy Security Policies](#)

You can define security-related policies and deploy them to the tenants that you choose. Use data gathered in Security Center to identify settings that matter most to you.

[Disconnect a Child Tenant from a Parent Tenant](#)

Sometimes you want to view a child tenant's data in a different parent tenant or stop viewing metrics from a child tenant. You can disconnect a child tenant from a parent tenant at any time. Disconnected child tenant data is retained, and visible when the child tenant is reconnected to a parent tenant.

[Security Center Metrics](#)

Security Center captures selected security, compliance, and governance metrics for all tenants.

Security Center Definitions

Keep these terms in mind when working with Security Center.

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions. Requires the Security Center add-on subscription.

Available in: Lightning Experience

Tenant

A virtual space provided to an individual customer of Salesforce.

Parent Tenant

A tenant used to view aggregated security data from multiple Salesforce tenants.

Child Tenant

A tenant that supplies data to a parent tenant.

Connected Tenants

Clusters of parent and child tenants.

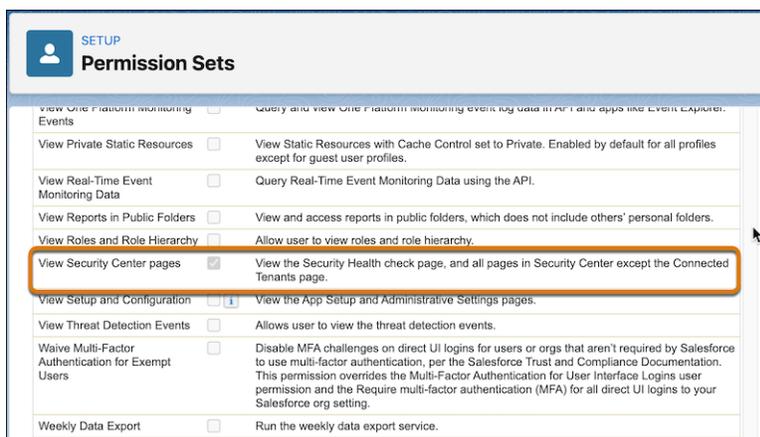
Enable Security Center Permissions

To give new users access to Security Center in the app launcher, enable Security Center permissions. You can assign Security Center permissions from Profiles or Permission Sets in Setup.

Enable Security Center permissions and features to streamline your admin security duties. To ensure that you can connect a child tenant to the parent tenant, make these updates in your parent and child orgs.

 **Note:** If any of the tabs in the Security Center App aren't available, review the Tab Settings section within your profile in Setup. Ensure that those tabs aren't set to Tab Hidden. Possible tabs include Dashboard, Connected Tenants, Alert Settings, Security Policies.

1. From Setup, click any Profile or Permission Set.
2. Under System Permissions, look for Manage Security Center and View Security Center pages. If a permission doesn't appear, contact your account representative to enable the Security Center license.



3. Click **Edit**.
4. Select **Manage Security Center** and **View Security Center pages**.
5. Save your changes.
6. To assign Permission Sets to users, add an assignment from Manage Assignments.
7. To ensure that you can connect a child tenant to the parent tenant, update the permissions to both the parent and child orgs.
8. If Security Center is enabled for production but you want it in a sandbox, see [Push Updated Licenses to Sandbox Orgs](#).

Designate a Parent Tenant in Security Center

To see security information for multiple tenants, designate a parent tenant to show data collected from that parent tenant and all connected child tenants. You can disconnect child tenants at any time. And you can group parent and child tenants based on their security policies or regulations.

Available in: **Enterprise, Performance, Unlimited**, and **Developer** Editions. Requires the Security Center add-on subscription.

Available in: Lightning Experience

EDITIONS

Available in: **Enterprise, Performance, Unlimited**, and **Developer** Editions.

Available in: Lightning Experience

USER PERMISSIONS

To view Security Center pages:

- View Security Center

To create and edit security policies:

- Manage Security Center

User Permissions Needed

To view Security Center pages and manage app configurations:	Manage Security Center (in parent and child tenants)
To complete the parent tenant and child tenant connection process:	API Enabled AND View Setup and Configuration AND View Roles and Role Hierarchy

Security Center is an application built on the Lightning Platform infrastructure. You can configure Security Center to copy customer data from a child tenant in one data center and then store the copied data in the parent tenant data center. You can connect child tenants in sandbox and production to a parent tenant in production. If a parent tenant is set up in a sandbox, you can only connect child tenants in sandboxes. Ensure that the Security Center license is enabled in parent and child tenants. Contact your account team for assistance. Because Security Center surfaces sensitive information, we recommend that you enable multi-factor authentication for all Security Center users.

 **Important:** This feature isn't supported in Government Cloud or Government Cloud Plus.

1. From the App Launcher in the tenant where you want to view aggregated security data, select **Security Center**.
2. On the Connected Tenants tab, if the parent tenant is in production, click **Connect Production Environment** or **Connect Sandbox Environment**. If the parent tenant is in a sandbox, click **Connect Tenant**.
3. On the login screen, enter the credentials for the child tenant that you want to connect. Child tenant credentials must be for a user who has these permissions: Manage Security Center, API Enabled, View Setup and Configuration, plus View Roles and Role Hierarchy.
4. Click **Log In**.
5. Salesforce asks you to confirm your authenticated connection. Click **Allow**.

The parent tenant is created and the Connected Tenant page shows the details of the child tenant that you added.

The Security Center app updates data elsewhere in the app only one time per day. Expect to see data from parent and child tenants in the app after the next app update.

 **Tip:** To ensure that Security Center displays accurate data for all connected tenants, reconnect each sandbox after you refresh it.

Security Center Data

Security Center offers several ways to view your security settings and data. Summary and Category dashboards organize aggregate data and totals for quick scanning. Detail pages show metric-specific trends and details about changes made to security settings on specific days. Security Center stores data for 6 months. Because Security Center surfaces sensitive information, we recommend that you enable multi-factor authentication for all Security Center users.

Available in: **Enterprise, Performance, Unlimited**, and **Developer** Editions. Requires the Security Center add-on subscription.

Available in: Lightning Experience

1. [Security Center Dashboards](#)

Security Center Summary and Category dashboards help you get a quick status update on your security posture and usage patterns. The Summary page organizes aggregate data for all security data metrics by category. Category dashboards show weekly data snapshots for all metrics in that category.

2. [Review Detailed Metric Data](#)

The metric detail page provides graphical and record-level views of changes, totals, and trends. Use this page for audits, deploying or updating policies, and monitoring usage patterns.

3. [Review Health Check Data](#)

The Health Check detail page in Security Center saves you time by aggregating multiple Health Check scores and settings in one place. From a parent tenant, you can see the average Health Check score for all connected tenants and individual tenant Health Check scores. Security Center stores Health Check settings for 6 months.

4. [Update Metric Data](#)

Security Center automatically updates data one time per day. If you want to update data more frequently, you can update most metrics on demand.

5. [Review Threat Detection Events](#)

The Threat Detection app in Security Center saves you time by aggregating information on detected threats to all your tenants in one place. From a parent tenant, see information on four types of detected events throughout your org in real time. Threat Detection uses statistical and machine learning methods powered by Event Monitoring to detect threats to your tenants. Security Center stores Threat Detection event information for 6 months.

Security Center Dashboards

Security Center Summary and Category dashboards help you get a quick status update on your security posture and usage patterns. The Summary page organizes aggregate data for all security data metrics by category. Category dashboards show weekly data snapshots for all metrics in that category.

Available in: **Enterprise, Performance, Unlimited**, and **Developer** Editions. Requires the Security Center add-on subscription.

Available in: Lightning Experience

USER PERMISSIONS

To view Security Center pages:

- View Security Center

Summary View

From the App Launcher, the default Summary view shows the aggregate data for all measured metrics. The three most sensitive metrics in each category appear. For more information, select a category.

Summary
View summary metrics for all connected tenants. To see details for a metric category, click the card title.

Authentication by Type				Configuration Metrics			
Metric	Value	Change	Last Updated	Metric	Value	Change	Last Updated
SSO	661 Logins	-6	8/02/2021, 11:59 PM	Managed Packages	1 Packages	0	8/03/2021, 08:31 AM
MFA & SSO	0 Logins	0	8/02/2021, 11:59 PM	Unmanaged Packages	1 Packages	0	8/03/2021, 08:31 AM
MFA, Username, & Password	0 Logins	0	8/02/2021, 11:59 PM	Connected Apps	1 Connected Apps	0	8/03/2021, 08:31 AM

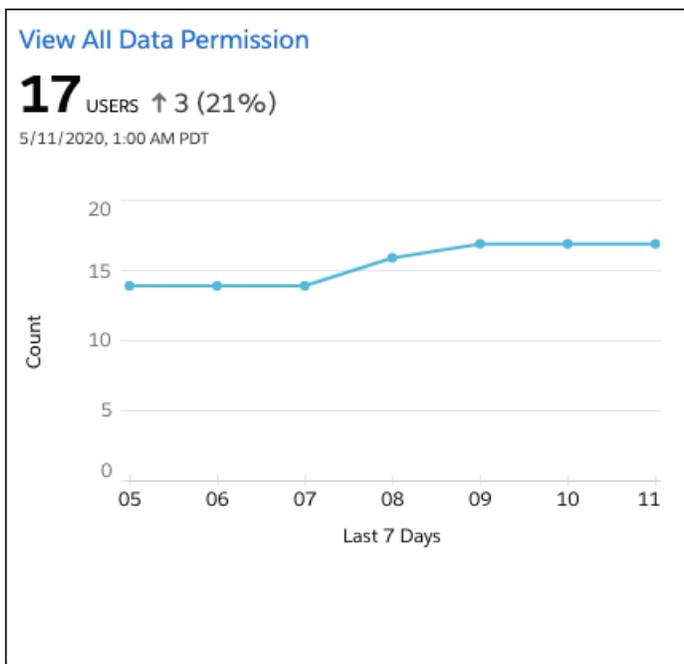
Permissions				User Metrics			
Metric	Value	Change	Last Updated	Metric	Value	Change	Last Updated
View All Data	3 Users	0	8/03/2021, 08:31 AM	No MFA	8 Users	0	8/03/2021, 08:31 AM
Modify All Data	3 Users	0	8/03/2021, 08:31 AM	Never Logged In	5 Users	0	8/03/2021, 08:31 AM
Manage Users	3 Users	0	8/03/2021, 08:31 AM	Inactive (90 Days)	0 Users	0	8/03/2021, 08:31 AM

Threat Detection			
Metric	Value	Change	Last Updated
Api Anomaly	- Threats	-	
Session Hijacking	- Threats	-	
Credential Stuffing	- Threats	-	
Report Anomaly	- Threats	-	

 **Note:** Review access to Security Center tabs if certain tabs aren't available including Dashboard, Connected Tenants, Alert Settings, and Security Policies.

Category Dashboard

Each metric category dashboard shows the most recent information. Metric cards show the most recent data for all connected tenants. Each card shows changes for the last 7 days and at the time of the last update via a line graph.



For more information, such as for an unexpected jump or drop in the chart, open the detail view for that metric and select the metric card name.

Review Detailed Metric Data

The metric detail page provides graphical and record-level views of changes, totals, and trends. Use this page for audits, deploying or updating policies, and monitoring usage patterns.

Available in: **Enterprise, Performance, Unlimited**, and **Developer** Editions. Requires the Security Center add-on subscription.

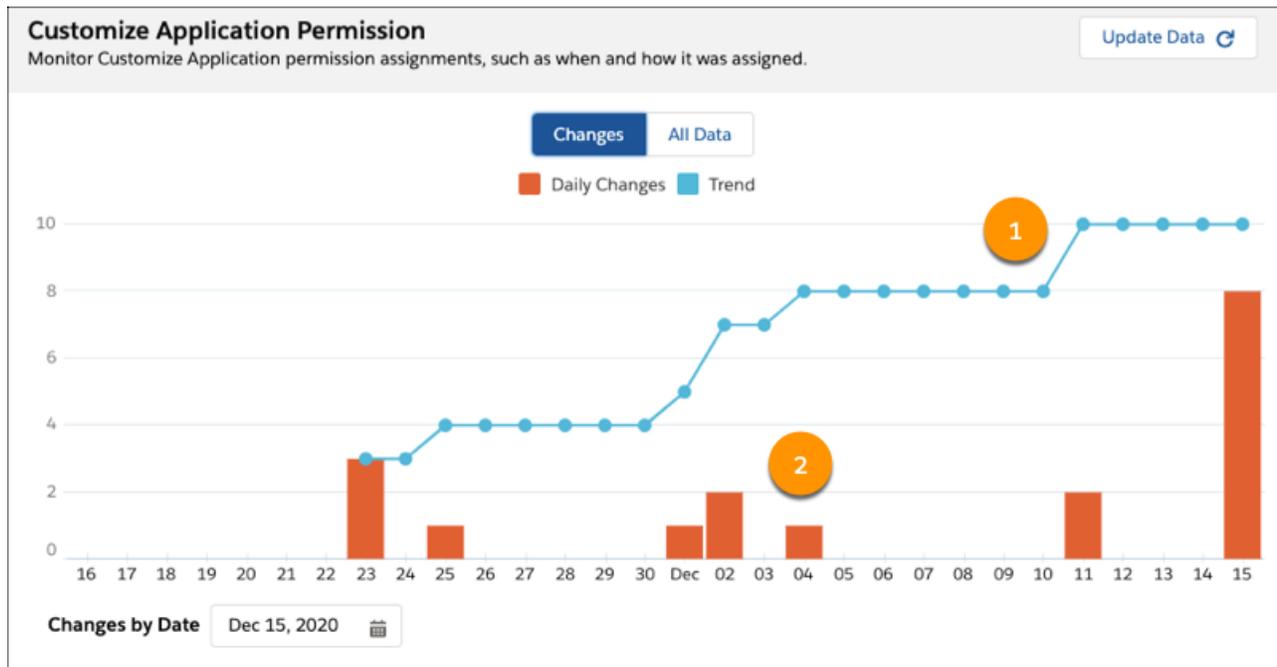
Available in: Lightning Experience

USER PERMISSIONS

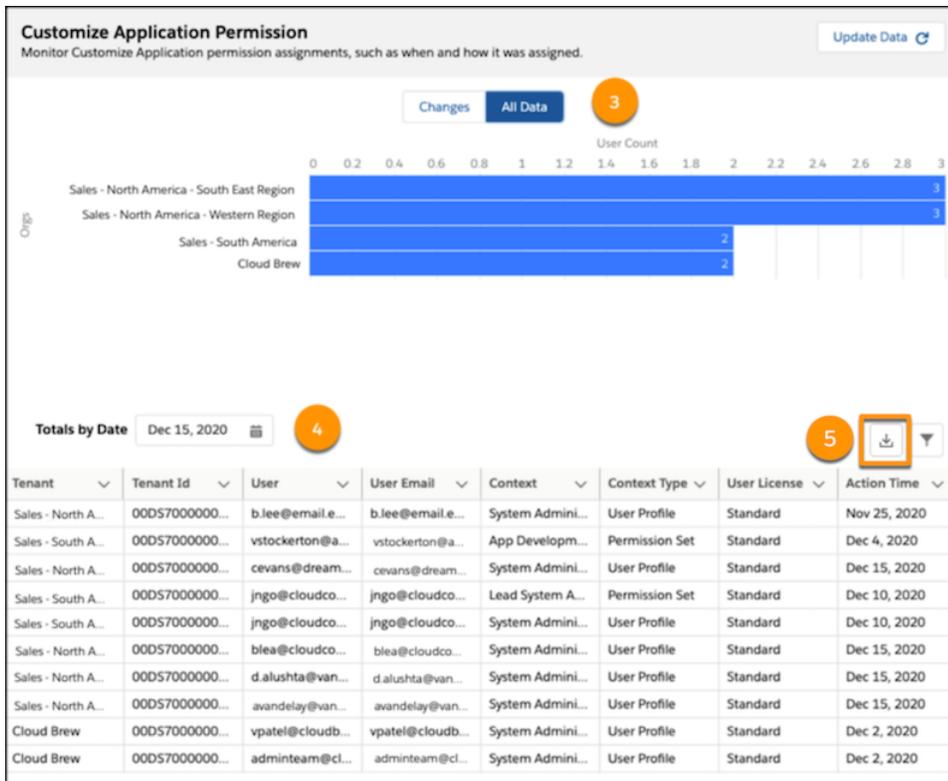
To view Security Center pages:

- View Security Center

Detail pages include these graphical elements.



- The trend graph offers an easy overview of the total metric count (1).
- The daily change graph isolates the changes made to a metric on a specific day (2).



The All Data view shows metric data by tenant (3). Detail pages also include a date range picker and detail record table (4). The detail record table is sortable, helping you organize by date, user, or the context around a particular change. You can also add custom filters to find data for specific tenants and users.

To download your data, click the Download icon (5).

 **Example:** Suppose you open the preceding detail view and see a jump in the number of users assigned the Customize Application permission. Because this permission is powerful, it's worth looking into. From the Changes By Date fields, select the days of the increase, and review the detail table. You can also click **All Data** to review how many users have the permission in each connected tenant. Several changes were made to permission sets on December 15, and some individuals were assigned the permission by the system admin. Use this data to inform your analysis of your security policies and practices. In this case, talk with the admin for the applicable tenants for a better understanding of how they apply your data access policies.

Detail View Considerations

Keep these considerations in mind as you review detail data.

- The Security Center shows up to 500 records per metric per tenant.
- Even though Security Center initiates its update daily, authentication metrics are recorded only for the previous day. For example, if an update starts at 8 AM GMT on April 23, it captures authentication metrics for April 22.
- On the Changes view, the detail table is visible for dates that record a change.
- The date displayed when you hover over a point in the All Data and Changes charts indicates the day Security Center picked up the change. This date is typically a maximum of 1 day after the change occurs. The date shown in the table below the chart reflects the day that the change actually occurred.
- You can create custom alerts to immediately learn about changes made to security settings. For more information, see [Create Alerts for Security Changes](#).

- Disconnecting or connecting tenants during the update period can cause partial data to load.
- Disruptions in the connection between Security Center and a tenant can lead to partial, incomplete, or missing detail record tables. If the Changes graph shows a change and you don't see a detail table, the app had a connection disruption during the update process. Graphs and detail record tables update during the next app update.

SEE ALSO:

[Create Alerts for Security Changes](#)

[Use Cases for Alerts](#)

Review Health Check Data

The Health Check detail page in Security Center saves you time by aggregating multiple Health Check scores and settings in one place. From a parent tenant, you can see the average Health Check score for all connected tenants and individual tenant Health Check scores. Security Center stores Health Check settings for 6 months.

Available in: **Enterprise, Performance, Unlimited**, and **Developer** Editions. Requires the Security Center add-on subscription.

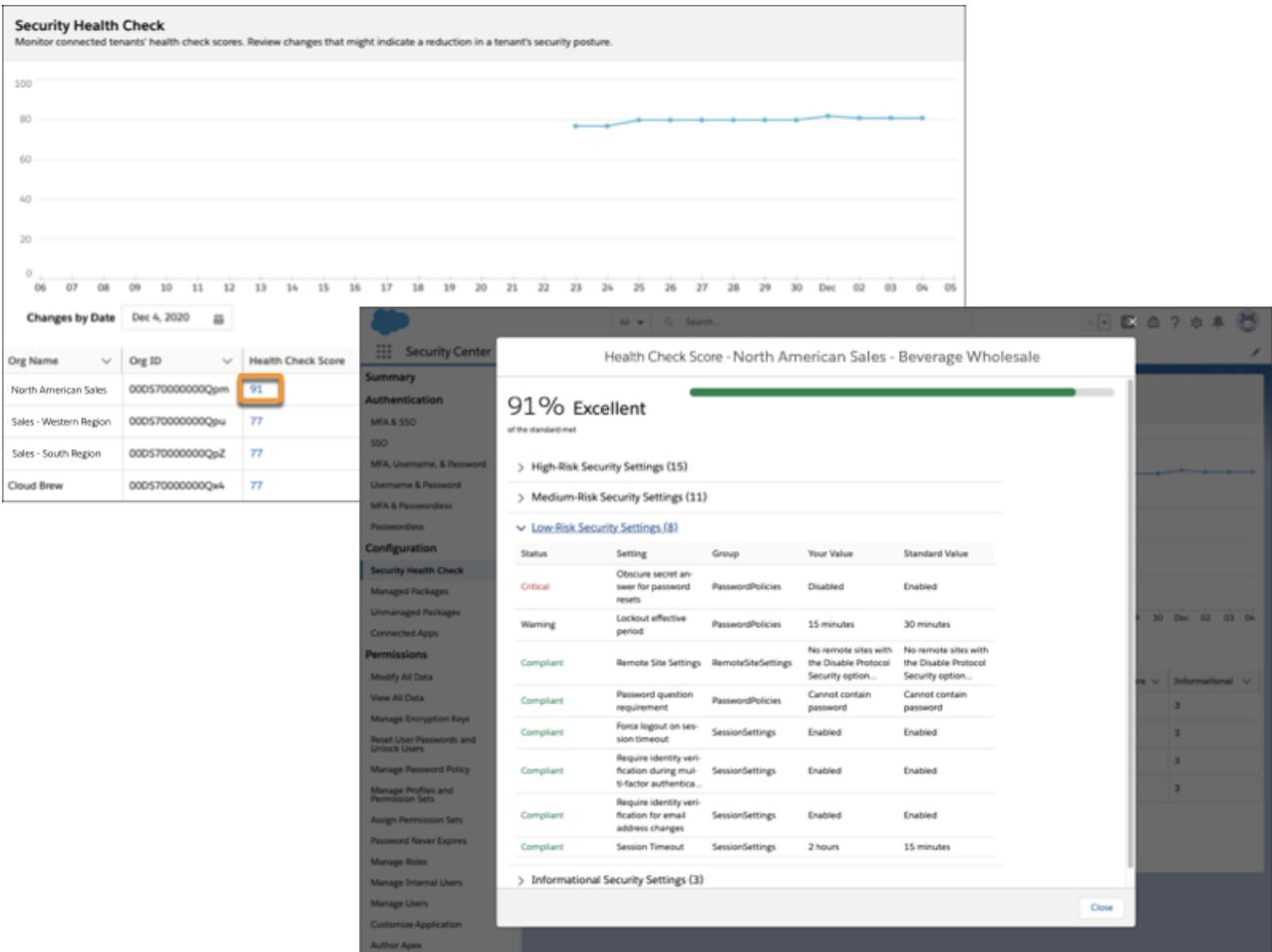
Available in: Lightning Experience

USER PERMISSIONS

To view Security Center pages:

- View Security Center

1. On the Summary page in the Security Center app, select the Configuration Metrics tile or **Configuration** in the navigation bar. The Configuration Metrics dashboard opens.
2. Click **Average Health Check Score**. The Security Health Check detail page opens. The time series chart shows the average Health Check score for all connected tenants for the last 30 days.
3. To see the Health Check scores that contributed to a day's average, enter a date in the Changes by Date field. A list view shows all Health Check scores for all connected tenants on that day. View risk scores by category, informational security setting counts, and per-tenant Health Check scores for all connected tenants. The Score Change Since Last Synced column shows whether a tenant's Health Check score rose, fell, or remained the same since the last app update.
4. To see what settings contributed to a specific tenant's Health Check score, select the value in that tenant's Health Check Score column. A window opens showing all of that tenant's High-Risk, Medium-Risk, Low-Risk, and Informational Security Settings for that day.



Example: Your organization has four tenants, and you want to see how your latest round of policy changes affects each tenant's Health Check score. Instead of signing in to each tenant, you log in to your Security Center parent tenant and scan the Health Check page. You see that a few of your tenants' Health Check scores fell by more than 10% since yesterday. It's possible that recent user or data access settings changes reduced those tenants' security postures. In this situation, you click those tenants Health Check Score values and review their settings. Now that you know which settings contribute to lower scores, you take this information to your security team and discuss adjusting your new policies.

Update Metric Data

Security Center automatically updates data one time per day. If you want to update data more frequently, you can update most metrics on demand.

Available in: **Enterprise, Performance, Unlimited**, and **Developer** Editions. Requires the Security Center add-on subscription.

Available in: Lightning Experience

USER PERMISSIONS

To view Security Center pages:

- View Security Center

Security Center takes a scheduled snapshot of data one time per day. The process can take a few hours to complete.

 **Note:** For Developer Edition orgs, assign at least one user with the Manage Security Center permission to collect metrics.

Table 6: Security Center Daily Update Schedule

Instance Region	Update Time
NA	8 am GMT
CS	8 am GMT
AP	4 pm GMT
EU	11 pm GMT
UM	11 pm GMT

 **Note:** You can also update individual metrics on-demand one time per hour.

1. In the Security Center app, navigate to a metric detail page.
2. Click **Update Data**.
Status lines show the time that the last update was initiated and how many tenants reported data.
3. At any time during an update, click the **tenant reporting** status link to see a list of tenants supplying updated information.
4. To view new data during and after an update, refresh the page.

Keep this information in mind when you update Security Center data.

- Metric updates made in a parent tenant also update the same metric data in all of that parent's child tenants, and vice versa.
- As a service protection, you can update data one time per hour.

Review Threat Detection Events

The Threat Detection app in Security Center saves you time by aggregating information on detected threats to all your tenants in one place. From a parent tenant, see information on four types of detected events throughout your org in real time. Threat Detection uses statistical and machine learning methods powered by Event Monitoring to detect threats to your tenants. Security Center stores Threat Detection event information for 6 months

Available in: **Enterprise, Performance, Unlimited**, and **Developer** Editions. Requires the Security Center and Event Monitoring add-on subscriptions.

Available in: Lightning Experience

USER PERMISSIONS

To view Security Center pages:

- View Security Center

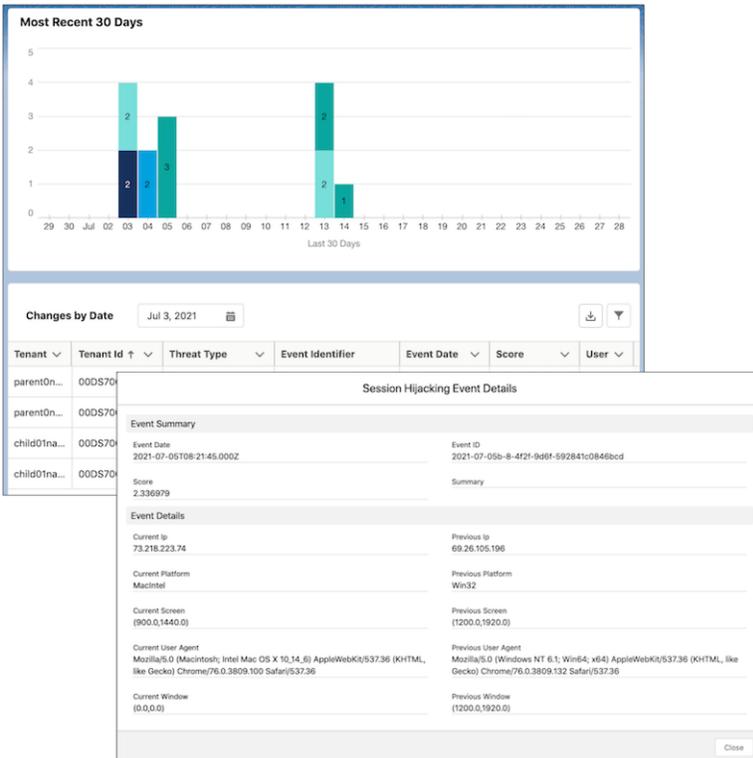
The Threat Detection app monitors your org for Credential Stuffing, API Anomaly, Session Hijacking, and Report Anomaly threat events. You can create an alert for any increases to the Threat Detection event count. For more information, see [Create Alerts for Security Changes](#). For more information on threat events, see [Threat Detection](#).

 **Note:** A delay of up to 1 day can occur between the time a threat event is observed by the Threat Detection app and the actual time of the threat event.

To review Threat Detection events, first enable streaming for these Threat Detection events from Event Manager in Setup.

- API Anomaly Event

- Credential Stuffing Event
 - Report Anomaly Event
 - Session Hijacking Event
1. On the Summary page in the Security Center app, select the Threat Detection tile. Or under the Monitoring category in the navigation bar, click **Threat Detection**.
 2. To see the detected events for a certain day, select a date in the Changes by Date field.
 3. Click the Event Identifier value of an event.
See information on when and where the event occurred, a summary of the event, and more.



 **Example:** You have multiple tenants and want to see if they've been targeted by malicious activity. Instead of signing in to each tenant, you log in to your Security Center parent tenant and scan the Threat Detection page. You see that a few Credential Stuffing events occurred on a certain day. It's possible that a user's login credentials were stolen and used to gain unauthorized access. In this situation, you click the Event Identifier values and review the event information. Use this information to educate your users on how they can create and manage strong passwords.

SEE ALSO:

- [Create Alerts for Security Changes](#)
- [Use Cases for Alerts](#)

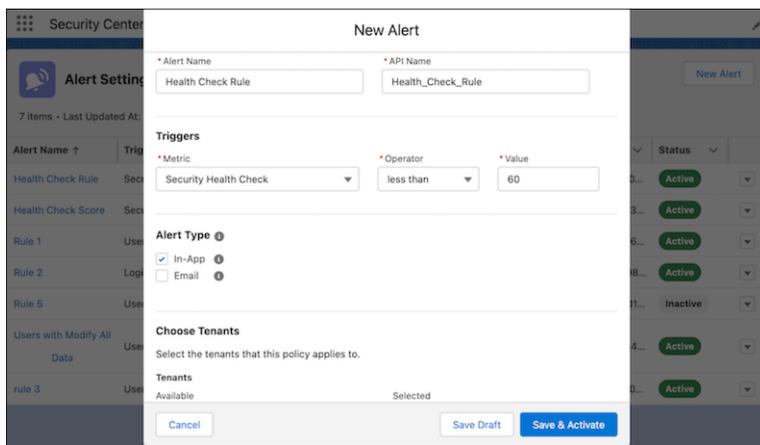
Create Alerts for Security Changes

Create custom alerts to immediately learn about changes made to security settings that you care about. Alerts notify you by email or in the Salesforce app when a setting in your Security Center tenant exceeds a threshold that you set. Create as many alerts as you want so that you can stay informed of your tenant's security posture.

 **Note:** You can automate processes for Security Center alerts with Salesforce Flow without having to select an alert type.

Customize your alerts to learn about changes to how your users log in, which permissions are assigned, and how many apps and managed package are installed. To create an alert:

1. From the Security Center dashboard, click the Alert Settings tab.
2. Click the **New Alert** button, then complete the fields. You can choose to receive one or both of the alert types.
3. When every field is complete, save the alert as a draft, or save and activate.



 **Example:** You track multiple connected tenants. Monitoring how many users have the Modify All Data permission is more difficult as your org grows. Instead of periodically checking the assigned permissions for each tenant, you can create an alert. Then you receive an email and an in-app notification so that you know when the total users with the Modify All Data permission exceeds your specified threshold or increases. With this information, you can reevaluate your tenant's security posture. You can also trigger a flow on the TenantSecurityNotification object for this alert to incorporate a custom business process. For more examples, see [Use Cases for Alerts](#) on page 908.

From the Alert Settings page, use the dropdown menu to activate, deactivate, or edit each alert. Click the name of an alert to see a history of when it was triggered.

[Use Cases for Alerts](#)

This page contains examples of custom alerts that you can create to monitor your tenant's security.

Use Cases for Alerts

This page contains examples of custom alerts that you can create to monitor your tenant's security.

Available in: Security Center is available in **Enterprise, Performance, Unlimited,** and **Developer** Editions as an add-on subscription.

EDITIONS

Available in: Security Center is available in **Enterprise, Performance, Unlimited,** and **Developer** Editions as an add-on subscription.

USER PERMISSIONS

To view Security Center pages:

- View Security Center

To create and edit Security Alerts:

- Manage Security Center

Threat Detection Score Alert

Set up a custom alert for Threat Detection events to ensure that you're notified of potential breaches in your tenant's security posture.



Example: More than one Threat Detection event can be a security risk. Create an alert for any increases to the Threat Detection event count so that you receive a notification whenever a Threat Detection event occurs. Trigger a flow on the TenantSecurityNotification object for this alert to create a Case record for the appropriate team to investigate. For more information, see [Threat Detection](#).

Managed Packages Alert

Gain visibility into who installs packages to maintain your tenant's security posture.



Example: Create an alert for managed package count increases to monitor who installs packages and when new packages are installed to determine a compliance or security threat. Trigger a flow on the TenantSecurityNotification object for this alert to create a record that's submitted to the appropriate approval process that all packages undergo.

Health Check Score Alert

Ensure that your Health Check score remains satisfactory with a custom alert.



Example: You want your Health Check score to consistently remain at 90% or above. Create a custom alert for Health Check Score decreases to ensure that you receive a notification whenever your score decreases. Then you can assess security threats and act to secure your tenant.

Inactive Users Alert

Monitor user activity to ensure security compliance and help keep your tenant secure.



Example: Create an alert for increases to the inactive users count to ensure that former employees don't have access to the tenant.

Permissions Alert

Instead of periodically checking the assigned permissions for each tenant, create an alert. With this information you can reevaluate your tenant's security posture.



Example: Monitoring how many users have the Modify All Data permission is more difficult as your tenant grows. Create an alert for this permission to receive a notification so that you know when the total users with the Modify All Data permission exceeds your specified threshold or increases. Trigger a flow on the TenantSecurityNotification object for this alert to integrate with an external security incident management system.

Define and Deploy Security Policies

You can define security-related policies and deploy them to the tenants that you choose. Use data gathered in Security Center to identify settings that matter most to you.

 **Note:** Deployed Security Policy settings overwrite existing settings in the target tenants.

To create a Security Policy:

1. On the Security Center dashboard, click the **Security Policies** tab, and then click **New Security Policy**.
2. Follow the prompts to define your policy, and then select the tenants that you want the policy to apply to.
3. Save the Security Policy as a draft, or save and activate it.
4. To view a policy's details, on the Security Policies tab, click the name of the policy.

EDITIONS

Available in: **Enterprise**, **Performance, Unlimited**, and **Developer** Editions. Requires the Security Center and Event Monitoring add-on subscriptions.

Available in: Lightning Experience

USER PERMISSIONS

To view Security Center pages:

- View Security Center

To create and edit security policies:

- Manage Security Center

New Security Policy



Trusted IP Ranges

Define trusted IP ranges for selected tenants.



Health Check Baseline

Define a Health Check Baseline for selected tenants.



Password Configuration

Define password requirements for selected tenants.



Session Settings

Define session details and timeout values for selected tenants.

Cancel
Next

 **Note:** The only tenants displayed for the mobile app security policy type are the connected tenants that are licensed for mobile app security.

 **Example:** Your business handles highly sensitive customer data, so you want to establish a Health Check Baseline with a higher risk setting than the Salesforce Baseline Standard. Create and upload a baseline to the Security Center, and deploy it to the relevant tenants.

You then decide that the baseline setting is too strict, so you make a new version of the policy. The updated Health Check Baseline is then applied to the same tenants as the original baseline.

On the Security Policies page, use the dropdown menu to activate, deactivate, or edit a policy. When you edit a policy, it saves as a new version. You can still change the settings in a specific tenant after a Security Policy is deployed to it.

Disconnect a Child Tenant from a Parent Tenant

Sometimes you want to view a child tenant's data in a different parent tenant or stop viewing metrics from a child tenant. You can disconnect a child tenant from a parent tenant at any time. Disconnected child tenant data is retained, and visible when the child tenant is reconnected to a parent tenant.

Available in: **Enterprise, Performance, Unlimited**, and **Developer** Editions. Requires the Security Center add-on subscription.

Available in: Lightning Experience

USER PERMISSIONS

To view Security Center pages and manage app configurations:

- Manage Security Center

Disconnecting a child tenant from a parent tenant affects your ability to view metric data.

- When you disconnect all child tenants from a parent tenant, the aggregate data in that parent tenant's dashboards and collected data is no longer visible.
 - To view data from a disconnected child tenant, reconnect it to any parent tenant. For example, a child tenant called Human Resources is disconnected from one parent tenant and connected to another parent tenant. The data for the Human Resources child tenant appears in the second parent tenant.
1. In a parent tenant, click the **Connected Tenants** tab.
 2. Find the child tenant you want to disconnect, and click **Disconnect**.
The Connected Tenants page updates and lists only the remaining child tenants. Security Center retains existing data from the disconnected child tenant in the background, but that data is no longer visible in the parent tenant.

Security Center Metrics

Security Center captures selected security, compliance, and governance metrics for all tenants.

Authentication Metrics

- External
- MFA & External
- MFA & OAuth
- MFA & Passwordless
- MFA & SSO

- MFA, Username, and Password
- OAuth
- Passwordless
- SSO
- Username & Password

Configuration Metrics

- Connected Apps
- Encryption Policies
- License Usage
- Login IP Ranges
- Managed Packages
- Mobile Security Policies
- Security Health Check
- Security Health Check Baselines
- Transaction Security Policy
- Trusted IP Ranges
- Unmanaged Packages

Permission Metrics

- API Only User Access
- Access Data Cloud Data Explorer
- Allows User Access Data Cloud
- Allows User Access Data Cloud Setup Menu
- Assign Permission Sets
- Author Apex
- Customize Application
- Download AppExchange Packages
- Edit Read Only Fields
- Enforce Enhanced Mobile App Security
- List Email Send
- Manage All Private Reports and Dashboards
- Manage Auth. Providers
- Manage Certificates
- Manage Connected Apps
- Manage Custom Permissions
- Manage Customer Users
- Manage Encryption Keys
- Manage Flow
- Manage Health Check

- Manage IP Addresses
- Manage Internal Users
- Manage Login Access Policies
- Manage Password Policies
- Manage Profiles and Permission Sets
- Manage Roles
- Manage Security Center
- Manage Session Permission Set Activations
- Manage Sharing
- Manage Users
- Mass Email
- Modify All Data
- Modify Data Classification
- Modify Metadata Through Metadata API Functions
- Password Never Expires
- Query All Files
- Reset Password
- Reset User Passwords and Unlock Users
- Send Email
- View All Custom Settings
- View All Data
- View All Users
- View Encrypted Data
- View Event Log Files
- View Security Center
- View Setup and Configuration
- Weekly Data Export

Monitoring Metrics

- Threat Detection

User and Profile Metrics

- Frozen Users
- Inactive (90 days)
- Never Logged In
- No MFA

Einstein Data Detect

Einstein Data Detect helps you identify sensitive data within your org so you can take steps to protect it. It uses native platform-native technology so that you don't rely on third-party services or port your data outside of Salesforce. Use Einstein Data Detect to expedite data categorization by aligning data sensitivity levels and categories to actual field data.

Compatibility

Einstein Data Detect is compatible with:

- AppExchange applications
- Sales Cloud
- Salesforce Industries
- Salesforce Platform
- Service Cloud
- Work.com

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** editions.

Requires the Salesforce Shield add-on subscription.

[Einstein Data Detect Glossary](#)

Familiarize yourself with common Einstein Data Detect terms.

[Install and Configure the Einstein Data Detect Managed Package](#)

Einstein Data Detect is a managed package that you can install in production and sandboxes. After you install the package, configure access controls to make sure that users can access it.

[Create a Data Detect Policy](#)

Data detect policies look for data patterns across fields and objects that you select. You can create multiple policies that help you find sensitive data that users inadvertently enter into fields across your org.

[Scan for Patterns with Einstein Data Detect](#)

Einstein Data Detect scans data based on your Data Detect policy settings. You can scan data in activated policies at any time.

[View and Classify Results with Einstein Data Detect](#)

You can view the aggregate results of completed scans and see a breakdown of the results by object and field. Results also include data classification assignments, which help you better understand your organization's data governance posture. See which fields aren't categorized and add or adjust a field's category based on the data detected. Data classifications are useful for reporting as well as creating Transaction Security and Shield Platform Encryption policies.

[Review Einstein Data Detect Scan Logs](#)

Einstein Data Detect scan logs offer insight into whether scans completed successfully. If a scan encountered an error or aborted unexpectedly, logs contain the error message and details about the issue.

Einstein Data Detect Glossary

Familiarize yourself with common Einstein Data Detect terms.

Scan

Einstein Data Detect's search process.

Data Detect Policy

A set of criterion governing Einstein Data Detect scans. Your policy contains all of the data patterns that you want the app to search for on each object.

Pattern

The data format that a scan looks for. For example, the social security number pattern looks for 9-digit numbers divided by hyphens into sections of 3, 2, and 4 integers.

Match

Values detected across one or more fields that meet pattern criteria.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** editions.

Requires the Salesforce Shield add-on subscription.

Install and Configure the Einstein Data Detect Managed Package

Einstein Data Detect is a managed package that you can install in production and sandboxes. After you install the package, configure access controls to make sure that users can access it.

Before installing the Einstein Data Detect package in production, make sure that My Domain is enabled.

 **Note:** To configure session security for government cloud organizations, make sure to deselect **Lock sessions to the IP address from which they originated** in Session Settings. For more information on configuring Session Security Settings, visit [Salesforce Help](#).

1. Go to the installation URL for Einstein Data Detect:
<https://sfdc.co/install-datadetect>.
2. Follow the standard process for installing a managed package.
3. Make sure that users who require access to Einstein Data Detect have the System Administrator user profile.
4. Give Einstein Data Detect users write access to the objects that you want them to scan. Scans initiated by a user only include objects that the user has write access to.

SEE ALSO:

[Salesforce Help: My Domain](#)

[Salesforce Help: Install a Package](#)

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** editions.

Requires the Salesforce Shield add-on subscription.

USER PERMISSIONS

To install managed packages:

- Download AppExchange Packages

Create a Data Detect Policy

Data detect policies look for data patterns across fields and objects that you select. You can create multiple policies that help you find sensitive data that users inadvertently enter into fields across your org.

1. In the Einstein Data Detect app, click the **Policies** tab.
2. Click **New**, and then enter a name for your policy. The name must be alphanumeric with no spaces or special characters.
3. Click **Save & Edit**.
4. At the top of the page, enter a policy description and click **Save**.

The screenshot shows the configuration page for a policy named 'SchedulingApp'. At the top, there are buttons for 'Unsaved Changes', 'Activate Policy', 'Scan', 'Save', and 'Delete'. The 'Save' button is highlighted with an orange box. Below the buttons, there is a 'Policy Name' field containing 'SchedulingApp' and a 'Description' field containing 'Look for sensitive data entered into the scheduling app.'.

5. Under Objects & Fields section, in the Objects pane, select an object. The object detail page opens with data pattern options and a list of the object's populated fields.
6.  **Tip:** Scanning large numbers of objects and fields can affect impact performance. Select only the patterns, objects, and fields you're most interested in.

By default, policies scan for all data patterns on all selected objects and fields. To narrow your search on specific patterns, deselect the patterns that you don't want.

7. In the field list, select **Add to Policy** for each field that you want to add.
8. To include the object's fields and pattern selections in future scans, set the object status to **Enable**. Only enabled objects are included in the scans execution. If you leave an object's status as **Disabled**, then it's not included in future scans. You can still save your pattern and field selections and enable them later.
9. Click **Save**.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** editions.

Requires the Salesforce Shield add-on subscription.

USER PERMISSIONS

To use Einstein Data Detect:

- Modify All Data
- AND
- API Enabled
- AND
- System Administrator

Object: Event 9 Save

Status
 Enabled 8

Data Patterns
 Select the data patterns you want scans to look for. 6

Credit Card Email URL IP Address Social Security Number

Quick Find

Field	Add to Policy	Field Owner	Compliance Categories	Sensitivity Level	Field Usage
Description (32000)	<input checked="" type="checkbox"/>	7			
DurationInMinutes	<input type="checkbox"/>				
EventSubtype (40)	<input type="checkbox"/>				
GroupEventType (40)	<input type="checkbox"/>				

10. Repeat steps 5–9 on other objects that you want to include in your policy. Your objects settings are added to your policy.

Scan for Patterns with Einstein Data Detect

Einstein Data Detect scans data based on your Data Detect policy settings. You can scan data in activated policies at any time.

1. On the Policy page, in the action menu for the policy you want to scan, click **Edit**.
2. On the policy's page, click **Activate Policy**.
3. Click **Scan**.
Einstein Data Detect looks for patterns specified by your policy. When the scan is finished, you can view the results on the Scan Results page.
4. To run another scans on the same policy, click **Deactivate Policy**. Then reactivate it and click **Scan**.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** editions.

Requires the Salesforce Shield add-on subscription.

USER PERMISSIONS

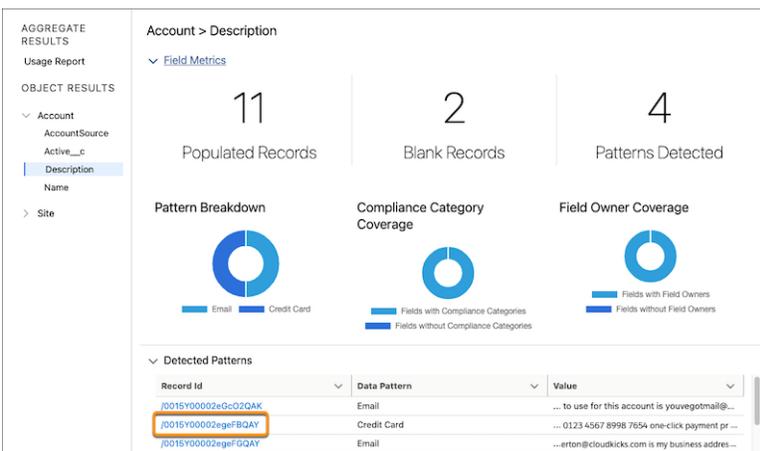
To use Einstein Data Detect:

- Modify All Data
- AND
- API Enabled
- AND
- System Administrator

View and Classify Results with Einstein Data Detect

You can view the aggregate results of completed scans and see a breakdown of the results by object and field. Results also include data classification assignments, which help you better understand your organization's data governance posture. See which fields aren't categorized and add or adjust a field's category based on the data detected. Data classifications are useful for reporting as well as creating Transaction Security and Shield Platform Encryption policies.

1. In the Einstein Data Detect app, select the **Results** tab.
2. Find the scan you want to see the results for. From the action menu, select **View**.
The Scan Results page opens with a dashboard showing the aggregated results of all objects and fields included in the policy.
3. To see aggregated results of all objects scanned, select **Aggregate Usage Report**.
The Usage Report dashboard shows how many objects, fields, and records were included in the policy's last scan. It also displays breakdowns of the patterns detected and how many fields have assigned compliance categories and field owners. Categories are based on [Data Classification metadata](#) values previously assigned to those fields.
4. To view results for each object, select an object from the panel.
5. Select a field from the panel.
A dashboard opens with field metrics, a list of detected patterns, and data classification sections.
If patterns are detected, the top 50 results are listed in the Data Patterns section. The record ID appears along with the pattern type that was found in the selected field. The table shows a portion of the sensitive value found along with the surrounding characters for context.
6. To view the record detail page for records, click the record ID.
A new tab opens, displaying information you can use to act on the sensitive data.



7. Expand the Data Classification section.
If the field has existing data classification assignments, those assignments appear. You can edit data classification assignments in this section, including assigning a field owner or changing compliance categories or sensitivity levels.

EDITIONS

Available in: Lightning Experience

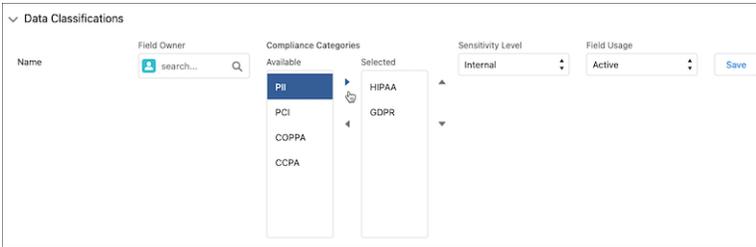
Available in: **Enterprise, Performance, Unlimited,** and **Developer** editions.

Requires the Salesforce Shield add-on subscription.

USER PERMISSIONS

To use Einstein Data Detect:

- Modify All Data
- AND
- API Enabled
- AND
- System Administrator



Review Einstein Data Detect Scan Logs

Einstein Data Detect scan logs offer insight into whether scans completed successfully. If a scan encountered an error or aborted unexpectedly, logs contain the error message and details about the issue.

1. In the Einstein Data Detect app, select the **Scan Logs** tab.
The page lists all scans.
2. To view a log, click a value in the Scan Log Number column.
A detail view opens showing information about the scan including the run ID, the policy ID, and other information about the policy and scan results. The Messages section shows the scan status and any errors.
3. If the Error Message field in the Message section includes an error, you can find more information in the log's related content.
 - a. Select the **Related** tab.
A list of the objects included in the policy appears.
 - b. If the Status column next to an object contains a value other than Success, select the object.
A detail page for the object opens, including a field for error messages.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** editions.

Requires the Salesforce Shield add-on subscription.

USER PERMISSIONS

To use Einstein Data Detect:

- **Modify All Data**
- AND
- API Enabled
- AND
- System Administrator

Strengthen Your Data's Security with Shield Platform Encryption

Shield Platform Encryption gives your data a whole new layer of security while preserving critical platform functionality. You can encrypt sensitive data at rest, and not just when transmitted over a network, so your company can confidently comply with privacy policies, regulatory requirements, and contractual obligations for handling private data.

 **Important:** Where possible, we changed noninclusive terms to align with our company value of Equality. We maintained certain terms to avoid any effect on customer implementations.

Shield Platform Encryption builds on the data encryption options that Salesforce offers out of the box. Data stored in many standard and custom fields and in files and attachments is encrypted using an advanced HSM-based key derivation system. So it's protected even when other lines of defense are compromised.

Your data encryption key material is never saved or shared across orgs. You can choose to have Salesforce generate key material for you or upload your own key material. By default, the Shield Key Management Service derives data encryption keys on demand from a master secret and your org-specific key material, and stores that derived data encryption key in an encrypted key cache. You can also opt out of key derivation on a key-by-key basis. Or you can store your final data encryption key outside of Salesforce and have the Cache-Only Key Service fetch it on demand from a key service that you control. No matter how you choose to manage your keys, Shield Platform Encryption secures your key material at every stage of the encryption process.

You can try out Shield Platform Encryption at no charge in Developer Edition orgs. It's available in sandboxes after it is provisioned for your production org.

 **Example:** Warren is an IT Systems Specialist for Northern Trail Outfitters, an outdoor apparel company. He must track the encryption policy status across the company's entire Salesforce rollout. He can simplify this process through the Security Center app, which can capture selected security metrics like encryption policies across the rollout. For more information, see [Take Charge of Your Security Goals with Security Center](#).

What You Can Encrypt

Shield Platform Encryption lets you encrypt a wide variety of standard fields and custom fields. You can also encrypt files and attachments stored in Salesforce, Salesforce search indexes, and more. We continue to make more fields and files available for encryption.

How Shield Platform Encryption Works

Shield Platform Encryption relies on a unique tenant secret that you control and a master secret that's maintained by Salesforce. By default, we combine these secrets to create your unique data encryption key. You can also supply your own final data encryption key. We use your data encryption key to encrypt data that your users put into Salesforce, and to decrypt data when your authorized users need it.

Set Up Your Encryption Policy

An encryption policy is your plan for encrypting data with Shield Platform Encryption. You can choose how you want to implement it. For example, you can encrypt individual fields and apply different encryption schemes to those fields. Or you can choose to encrypt other data elements such as files and attachments, data in Chatter, or search indexes. Remember that encryption is not the same thing as field-level security or object-level security. Put those controls in place before you implement your encryption policy.

Filter Encrypted Data with Deterministic Encryption

You can filter data that's protected with Shield Platform Encryption using deterministic encryption. Your users can filter records in reports and list views, even when the underlying fields are encrypted. You can apply case-sensitive deterministic encryption or exact-match case-insensitive deterministic encryption to data on a field-by-field basis.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

[Key Management and Rotation](#)

Shield Platform Encryption lets you control and rotate the key material used to encrypt your data. You can use Salesforce to generate a tenant secret for you, which is then combined with a per-release master secret to derive a data encryption key. This derived data encryption key is then used in encrypt and decrypt functions. You can also use the Bring Your Own Key (BYOK) service to upload your own key material, or store key material outside of Salesforce and have the Cache-Only Key Service fetch your key material on demand.

[Shield Platform Encryption Customizations](#)

Some features and settings require adjustment before they work with encrypted data.

[Tradeoffs and Limitations of Shield Platform Encryption](#)

A security solution as powerful as Shield Platform Encryption doesn't come without some tradeoffs. When your data is encrypted, some users may see limitations to some functionality, and a few features aren't available at all. Consider the impact on your users and your overall business solution as you design your encryption strategy.

SEE ALSO:

[Learning Map: Shield Learning Map](#)

[Take Charge of Your Security Goals with Security Center](#)

What You Can Encrypt

Shield Platform Encryption lets you encrypt a wide variety of standard fields and custom fields. You can also encrypt files and attachments stored in Salesforce, Salesforce search indexes, and more. We continue to make more fields and files available for encryption.

[Which Standard Fields Can I Encrypt?](#)

You can encrypt certain fields on standard and custom objects, data in Chatter, and search index files. With some exceptions, encrypted fields work normally throughout the Salesforce user interface, business processes, and APIs.

[Which Custom Fields Can I Encrypt?](#)

You can apply Shield Platform Encryption to the contents of fields that belong to one of these custom field types.

[Which Files Are Encrypted?](#)

When you enable Shield Platform Encryption for files and attachments, all files and attachments that can be encrypted are encrypted. The body of each file or attachment is encrypted when it's uploaded.

[What Other Data Elements Can I Encrypt?](#)

In addition to standard and custom field data and files, Shield Platform Encryption supports other Salesforce data. You can encrypt CRM Analytics datasets, Chatter fields, fields in the Salesforce B2B Commerce managed package, and more.

SEE ALSO:

[Strengthen Your Data's Security with Shield Platform Encryption](#)

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Which Standard Fields Can I Encrypt?

You can encrypt certain fields on standard and custom objects, data in Chatter, and search index files. With some exceptions, encrypted fields work normally throughout the Salesforce user interface, business processes, and APIs.

When you encrypt a field, existing values aren't encrypted immediately. Values are encrypted only after they're touched or after they're synchronized with the latest encryption policy. Synchronize existing data with your policy from Setup on the Encryption Statistics page.

Compatible Standard Fields

You can encrypt the contents of these standard field types.

Object	Fields	Notes
Account Participant	Comments	The Account Participant object is available in select Salesforce Industries products.
Accounts	Account Name Account Site Billing Address (encrypts Billing Street and Billing City) Description Fax Phone Shipping Address (encrypts Shipping Street and Shipping City) Website	If you enabled Person Accounts, certain account and contact fields are combined into one record. In that case, you can enable encryption for a different set of Account fields.
Accounts with Person Accounts enabled	Account Name Account Site Assistant Assistant Phone Billing Address (encrypts Billing Street and Billing City) Description Email Fax Home Phone Mailing Address (encrypts Mailing Street and Mailing City) Mobile	

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Object	Fields	Notes
	Other Address (encrypts Other Street and Other City) Other Phone Phone Shipping Address (encrypts Shipping Street and Shipping City) Title Website	
Activity	Description (encrypts Event—Description and Task—Comment) Subject (encrypts Event—Subject and Task—Subject)	Selecting an Activity field encrypts that field on standalone events, event series (Lightning Experience), and recurring events (Salesforce Classic).
AI Natural Language Process Chunk Result	Additional Information Response	
AI Natural Language Process Result	Additional Information Response	
Applicant	Submission Date	
Application Form	Birth Date Email First Name Last Name Middle Name Phone Prefix Suffix Unique Reference Number	
Assessment Question Response	Choice Value Date Value Date Time Value Response Text Response Value	
Authorization Form	Name	

Object	Fields	Notes
Authorization Form Consent	Name	
Authorization Form Data Use	Name	
Authorization Form Text	Name	
Business License	Identifier	Emergency Response Management for Public Sector standard objects and fields are available to users who have the Emergency Response for Public Sector permission set license.
Business License Application	Site Address (encrypts Site Street and Site City)	
Business Profile	Business Operating Name Business Tax Identifier	
Cases	Description Subject	
Case Comments	Body (including internal comments)	
Chat Transcript	Body Supervisor Transcript Body	Before you can apply encryption to Chat fields, add the Supervisor Transcript Body field to the LiveChatTranscript record home layout.
Contact Point Address	Address	
Contact Point Email	Email address	
Contact Point Phone	Telephone number	
Contacts	Assistant Assistant Phone Description Email Fax Home Phone Mailing Address (encrypts Mailing Street and Mailing City) Mobile Name (encrypts First Name, Middle Name, and Last Name) Other Address (encrypts Other Street and Other City) Other Phone Phone Title	

Object	Fields	Notes
Contracts	Billing Address (encrypts Billing Street and Billing City) Shipping Address (encrypts Shipping Street and Shipping City)	
Conversation Context Entry	Key Value	
Conversation Entry	Actor Name Message	
Conversation Participant	Participant Display Name	
Course Offering	Name	Emergency Response Management for Public Sector standard objects and fields are available to users who have the Emergency Response for Public Sector permission set license.
Custom Objects	Name	
Email Messages	From Name From Name To Address CC Address BCC Address Subject Text Body HTML Body Headers	If you use Email-to-Case, these fields are also encrypted on the customer emails that generate cases.
Email Message Relations	Relation Address	
Flow Orchestration Work Item	Screen Flow Inputs	
Identity Document	Document Number Expiration Date Issue Date	
Individual	Name	The Individual object is available only if you enable the setting to make data protection details available in records.
Leads	Address (Encrypts Street and City)	

Object	Fields	Notes
	Company Description Email Fax Mobile Name (Encrypts First Name, Middle Name, and Last Name) Phone Title Website	
List Emails	From Name From Address Reply To Address	
List Email Sent Results	Email	
Messaging End User	Messaging Platform Key Name Profile Picture URL	
OCR Document Scan Result	Extracted Values	
OCR Scan Result Template Mapping	Mapped Fields	
Opportunities	Description Next Step Opportunity Name	
Opportunity Participant	Comments	The Opportunity Participant object is available in select Salesforce Industries products.
Payment Instrument	Bank Account Name	—
Public Complaint	Business Address Business Name Email First Name Last Name Mobile Number	Emergency Response Management for Public Sector standard objects and fields are available to users who have the Emergency Response for Public Sector permission set license.

Object	Fields	Notes
Recommendations	Description	
Referral	Client Email Client Name Client Phone Provider Email Provider Name Provider Phone Referrer Email Referrer Name Referrer Phone	
Regulatory Code Violation	Corrective Action Description Description	Emergency Response Management for Public Sector standard objects and fields are available to users who have the Emergency Response for Public Sector permission set license.
Service Appointments	Address (Encrypts Street and City) Description Subject	
Social Persona	Bio Profile URL Provider External Picture URL Real Name	Before you can apply encryption to Social Persona fields, make sure that Social Customer Service is enabled and connected to a Marketing Cloud Social service.
Social Post	Attachment URL Headline Message Post URL Social Handle	Before you can apply encryption to Social Post fields, make sure that Social Customer Service is enabled and connected to a Marketing Cloud Social service.
Survey Question Response	Date Value Date Time Value Choice Value Response Value	

Object	Fields	Notes
Training Course	Description Name	Emergency Response Management for Public Sector standard objects and fields are available to users who have the Emergency Response for Public Sector permission set license.
User	Email	
Utterance Suggestion	Utterance	
Video Call	Description End Date Time Start Date Time Vendor Meeting Uuid	
Video Call Participant	Email Join Date Time Leave Date Time	
Violation Enforcement Action	Description	Emergency Response Management for Public Sector standard objects and fields are available to users who have the Emergency Response for Public Sector permission set license.
Voice Call	FromPhoneNumber ToPhoneNumber	
Web Quote	Introduction Notes Ship to City Ship to Country Ship to Name Ship to Postal Code Ship to State Ship to Street Description Product Code	
Work Orders	Address (Encrypts Street and City) Description Subject	

Object	Fields	Notes
Work Order Line Items	Address (Encrypts Street and City) Description Subject	

Compatible Automotive Cloud Fields

Automotive Cloud standard objects and fields are available to users who have the Automotive Foundation User and the Vehicle and Asset Finance permission sets.

Object	Fields
Financial Account	Financial Account Number Name

Compatible Health Cloud Fields

Health Cloud standard objects and fields are available to users who have the Health Cloud Platform permission set license.

 **Note:** Deterministic encryption is unavailable for long text fields and fields that have Notes in the name.

Object	Fields
Care Plan Template Problem	Name
Care Program Enrollee	Name
Care Program Enrollee Product	Name
Care Program Provider	Name
Care Request	Admission Notes Disposition Notes Facility Record Number First Reviewer Notes Medical Director Notes Member First Name Member Last Name Member ID Member Group Number Resolution Notes

Object	Fields
	Root Cause Notes
Care Request Drug	Prescription Number
Care Specialty	Name
Contact Encounter	Name
Coverage Benefit	Benefit Notes Coinsurance Notes Copoly Notes Deductible Notes Lifetime Maximum Notes Name Out-of-Pocket Notes Source System Identifier
Coverage Benefit Item	Coverage Level Notes Service Type Service Type Code Source System Identifier
Healthcare Provider Specialty	Name
Healthcare Provider Treated Condition	Name
Member Plan	Affiliation Group Number Issuer Number Member Number Name Primary Care Physician Source System Identifier
Purchaser Plan	Name

Compatible Financial Services Cloud Fields

Financial Services Cloud standard objects and fields are available to users who have Financial Services Cloud enabled.

Object	Fields
Financial Deal	Description Financial Deal Code Name
Interaction	Comment Name
Interaction Attendee	Email Address
Interaction Summary	Comment
Interaction Related Account	Comment
Interaction Summary	Next Steps Meeting Notes Title
Interaction Summary Discussed Account	Comment

Compatible Grantmaking Fields

Grantmaking standard objects and fields are available to users who have Grantmaking enabled.

Object	Fields
Budget Participant	Comments
Funding Award Participant	Comments
Funding Opportunity Participant	Comments
Individual Application Participant	Comments

Compatible Insurance for Financial Services Cloud Fields

Insurance for Financial Services Cloud standard objects and fields are available to users who have Financial Services Cloud enabled.

Object	Fields
Business Milestone	Milestone Description Milestone Name
Claim	Claim Number Incident Site Report Number

Object	Fields
Customer Property	Address Lien Holder Name
Insurance Policy	Policy Number Servicing Office Universal Policy Number
Person Life Event	Event Description Event Name
Securities Holding	Name

Compatible Loyalty Management Fields

Loyalty Management standard objects and fields are available to users who have Loyalty Management enabled.

Shield Platform Encryption Supported Objects	Fields
Loyalty Program Group Member Relationship	Member Name

Compatible Nonprofit Cloud Fields

Nonprofit Cloud standard objects and fields are available to users who have Nonprofit Cloud features enabled.

Object	Fields
Gift Entry	City Country Email Expiry Month Expiry Year First Name Home Phone Last 4 Last Name Mobile Phone Organization Name State/Province Street

Object	Fields
Payment Instrument	Bank Account Number

Compatible Salesforce CPQ Fields

Salesforce CPQ standard objects and fields are available to users who have the Salesforce CPQ permission set license.

Object	Fields
Lookup Data	Lookup Data
Process Input Value	Value
Quote	Bill To City Bill To Country Bill To Name Bill To Postal Code Bill To State Bill To Street Introduction Notes Ship To City Ship To Country Ship To Name Ship To Postal Code Ship To State Ship To Street
Quote Template	Company Name
Quote Term	Body
Tax Exemption Certificate	Certificate Number Country County Exempt Company Name Notes Postal Code State Street Address Street Address_2

Compatible Workplace Command Center Fields

Object	Fields	Notes
Employee	Alternate Email Email First Name Home Address Home Phone Last Name Middle Name Preferred First Name Work Phone	To enable encryption on the Employee object, contact Salesforce Customer Support.

Which Custom Fields Can I Encrypt?

You can apply Shield Platform Encryption to the contents of fields that belong to one of these custom field types.

- Email
- Phone
- Text
- Text Area
- Text Area (Long)
- Text Area (Rich)
- URL
- Date
- Date/Time

After a custom field is encrypted, you can't change the field type. For custom phone and email fields, you also can't change the field format.

! **Important:** When you encrypt the Name field, enhanced lookups are automatically enabled. Enhanced lookups improve the user's experience by searching only through records that have been looked up recently, and not all existing records. Switching to enhanced lookups is a one-way change. You can't go back to standard lookups, even if you disable encryption.

You can't use Schema Builder to create an encrypted custom field.

To encrypt custom fields that have the `Unique` or `External ID` attribute, you can only use deterministic encryption.

Unsupported Custom Fields

Some custom fields can't be encrypted.

- Fields on external data objects
- Fields that are used in an account contact relation
- Fields with data translation enabled
- Rich Text Area fields on Knowledge Articles

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

Which Files Are Encrypted?

When you enable Shield Platform Encryption for files and attachments, all files and attachments that can be encrypted are encrypted. The body of each file or attachment is encrypted when it's uploaded.

These kinds of files are encrypted when you enable file encryption:

- Files attached to email
- Files attached to feeds
- Files attached to records
- Images included in Rich Text Area fields
- Files on the Content, Libraries, and Files tabs (Salesforce Files, including file previews, and Salesforce CRM Content files)
- Files managed with Salesforce Files Sync and stored in Salesforce
- Files attached to Chatter posts, comments, and the sidebar
- Notes body text using the new Notes tool
- Files attached to Knowledge articles
- Quote PDFs

These file types and attachments aren't encrypted:

- Chatter group photos
- Chatter profile photos
- Documents
- Notes previews in the new Notes tool
- Notes and Notes previews in the old Notes tool

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

What Other Data Elements Can I Encrypt?

In addition to standard and custom field data and files, Shield Platform Encryption supports other Salesforce data. You can encrypt CRM Analytics datasets, Chatter fields, fields in the Salesforce B2B Commerce managed package, and more.

Change Data Capture

Change Data Capture provides near-real-time changes of Salesforce records, enabling you to synchronize corresponding records in an external data store. If a Salesforce record field is encrypted with Shield Platform Encryption, changes to encrypted field values generate change events. You can encrypt these change events by selecting **Encrypt and deliver Change Data Capture events** on the Encryption Policy page in Setup.

Chatter Feed

Encrypted Chatter data includes data in feed posts and comments, questions and answers, link names and URLs. It also includes poll choices and questions, and content from your custom rich publisher apps.

EDITIONS

Available as an add-on subscription in: **Enterprise, Performance, and Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

EDITIONS

Available as an add-on subscription in: **Enterprise, Performance, and Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

The revision history of encrypted Chatter fields is also encrypted. If you edit or update an encrypted Chatter field, the old information remains encrypted.

Chatter data is stored in the Feed Attachment, Feed Comment, Feed Poll Choice, Feed Post, and Feed Revision objects. The database fields on these objects that house encrypted data is visible from the Encryption Statistics page in Setup.

- ChatterExtensionInstance—Payload
- ChatterExtensionInstance—PayloadVersion
- ChatterExtensionInstance—TextRepresentation
- ChatterExtensionInstance—ThumbnailUrl
- ChatterExtensionInstance—Title
- FeedAttachment—Title
- FeedAttachment—Value
- FeedComment—RawCommentBody
- FeedPollChoice—ChoiceBody
- FeedPost—LinkUrl
- FeedPost—RawBody
- FeedPost—Title
- FeedRevision—RawValue

Some fields listed in the Encryption Statistics aren't visible in the UI by the same name. However, they store all encrypted data that's visible in the UI.

 **Note:** Enabling Encryption for Chatter encrypts all eligible Chatter fields. You can't choose to encrypt only some Chatter fields.

CRM Analytics

Encrypts new CRM Analytics datasets.

 **Note:** Data that was in CRM Analytics before encryption was enabled isn't encrypted. If existing data is imported from Salesforce objects through the dataflow, the data becomes encrypted on the next dataflow run. Other existing data (such as CSV data) must be reimported to become encrypted. Although existing data isn't encrypted, it's still accessible and fully functional in its unencrypted state when encryption is enabled.

Salesforce B2B Commerce

Shield Platform Encryption for B2B Commerce (version 4.10 and later) adds an extra layer of security to the data your customers enter in Salesforce B2B Commerce ecommerce storefronts. For a list of the supported fields, see [Shield Platform Encryption for B2B Commerce](#).

Search Indexes

When you encrypt search indexes, each file created to store search results is encrypted.

How Shield Platform Encryption Works

Shield Platform Encryption relies on a unique tenant secret that you control and a master secret that's maintained by Salesforce. By default, we combine these secrets to create your unique data encryption key. You can also supply your own final data encryption key. We use your data encryption key to encrypt data that your users put into Salesforce, and to decrypt data when your authorized users need it.

 **Important:** Where possible, we changed noninclusive terms to align with our company value of Equality. We maintained certain terms to avoid any effect on customer implementations.

Encrypting files, fields, and attachments has no effect on your org's storage limits.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

[Shield Platform Encryption Terminology](#)

Encryption has its own specialized vocabulary. To get the most out of your Shield Platform Encryption features, it's a good idea to familiarize yourself with key terminology.

[What's the Difference Between Classic Encryption and Shield Platform Encryption?](#)

With Shield Platform Encryption, you can encrypt a variety of widely used standard fields, along with some custom fields and many kinds of files. Shield Platform Encryption also supports person accounts, cases, search, approval processes, and other key Salesforce features. Classic encryption lets you protect only a special type of custom text field, which you create for that purpose.

[Behind the Scenes: The Shield Platform Encryption Process](#)

When users submit data, the application server looks for the org-specific data encryption key in its cache. If it isn't there, the application server gets the encrypted tenant secret from the database and asks the key derivation server to derive the key. The Shield Platform Encryption service then encrypts the data on the application server. If customers opt out of key derivation or use the Cache-Only Key Service, the encryption service applies the customer-supplied data encryption key directly to customer data.

[Behind the Scenes: The Search Index Encryption Process](#)

The Salesforce search engine is built on the open-source enterprise search platform software Apache Solr. The search index, which stores tokens of record data with links back to the original records stored in the database, is housed within Solr. Partitions divide the search index into segments to allow Salesforce to scale operations. Apache Lucene is used for its core library.

[How Does Shield Platform Encryption Work in a Sandbox?](#)

Refreshing a sandbox from a production org creates an exact copy of the production org. If Shield Platform Encryption is enabled on the production org, all encryption settings are copied, including tenant secrets created in production.

[Why Bring Your Own Key?](#)

Shield Platform Encryption's Bring Your Own Key (BYOK) feature gives you an extra layer of protection if there is unauthorized access to critical data. It could also help you meet the regulatory requirements that come with handling financial data, such as credit card numbers; health data, such as patient care records or insurance information; or other kinds of private data, such as social security numbers, addresses, and phone numbers. After you've set up your key material, you can use Shield Platform Encryption as you normally would to encrypt data at rest in your Salesforce org.

[Why Isn't My Encrypted Data Masked?](#)

If the Shield Platform Encryption service isn't available, data is masked in some types of encrypted fields. This is to help you troubleshoot encryption key issues, not to control user access to data. If you have data that you don't want some users to see, revisit those users' field-level security settings, record access settings, and object permissions.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

[Shield Platform Encryption in Hyperforce](#)

Shield Platform Encryption operates in parallel with volume-level encryption. By default, Hyperforce provides volume-level encryption for data at rest. Volume-level encryption protects all the data on a disk with one encryption key, which Salesforce owns and manages. With Shield Platform Encryption, you can encrypt your data in Hyperforce with unique keys that you control and manage.

[How Do I Deploy Shield Platform Encryption?](#)

When you deploy Shield Platform Encryption to your org with a tool such as Salesforce Extensions for Visual Studio Code, Migration Tool, or Postman, the Encrypted field attribute persists. However, if you deploy to orgs with different encryption settings, the effect depends on whether Shield Platform Encryption is enabled in the target org.

SEE ALSO:

[Strengthen Your Data's Security with Shield Platform Encryption](#)

Shield Platform Encryption Terminology

Encryption has its own specialized vocabulary. To get the most out of your Shield Platform Encryption features, it's a good idea to familiarize yourself with key terminology.

 **Important:** Where possible, we changed noninclusive terms to align with our company value of Equality. We maintained certain terms to avoid any effect on customer implementations.

Data Encryption

The process of applying a cryptographic function to data that results in ciphertext. The Shield Platform Encryption process uses symmetric key encryption, a 256-bit Advanced Encryption Standard (AES) algorithm using CBC mode, and a randomized 128-bit initialization vector to encrypt data stored on the Salesforce Platform. Both data encryption and decryption occur on the application servers.

Data Encryption Keys

Shield Platform Encryption uses data encryption keys to encrypt and decrypt data. Data encryption keys are derived on the Shield Key Management Service (KMS) using keying material split between a per-release master secret and an org-specific tenant secret stored encrypted in the database. The 256-bit derived keys exist in memory until evicted from the cache.

Encrypted Data at Rest

Data that is encrypted when persisted on disk. Salesforce supports encryption for fields stored in the database; documents stored in files, content, libraries, and attachments; search index files; CRM Analytics datasets; and archived data.

Encryption Key Management

Refers to all aspects of key management, such as key generation, processes, and storage. Administrators or users who have the Manage Encryption Keys permission can work with Shield Platform Encryption key material.

Hardware Security Module (HSM)

Used to provide cryptography processing and key management for authentication. Shield Platform Encryption uses HSMs to generate and store secret material, and run the function that derives data encryption keys used by the encryption service to encrypt and decrypt data.

Initialization Vector (IV)

A random sequence used with a key to encrypt data.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Shield Key Management Service (KMS)

Generates, wraps, unwraps, derives, and secures key material. When deriving key material, the Shield KMS uses a pseudorandom number generator and input such as a password to derive keys. Shield Platform Encryption uses PBKDF2 (Password-based Key Derivation Function 2) with HMAC-SHA-256.

Key Rotation

The process of generating a new tenant secret and archiving the previously active one. Active tenant secrets are used for both encryption and decryption. Archived ones are used only for decryption until all data has been re-encrypted using the new, active tenant secret.

Master HSM

The master HSM consists of a USB device used to generate secure, random secrets each Salesforce release. The master HSM is air-gapped from Salesforce's production network and stored securely in a bank safety deposit box.

Master Secret

Used with the tenant secret and key derivation function to generate a derived data encryption key (customers can opt out of key derivation). The master secret is rotated each release by Salesforce and encrypted using the per-release master wrapping key. The master wrapping key is in turn encrypted with the Shield KMS's public key so it can be stored encrypted on the file system. Only HSMs can decrypt it. *No Salesforce employees have access to these keys in cleartext.*

Master Wrapping Key

A symmetric key is derived and used as a master wrapping key, also known as a key wrapping key, encrypting all the per-release keys and secrets bundle.

Tenant Secret

An organization-specific secret used in conjunction with the master secret and key derivation function to generate a derived data encryption key. *No Salesforce employees have access to these keys in cleartext.*

What's the Difference Between Classic Encryption and Shield Platform Encryption?

With Shield Platform Encryption, you can encrypt a variety of widely used standard fields, along with some custom fields and many kinds of files. Shield Platform Encryption also supports person accounts, cases, search, approval processes, and other key Salesforce features. Classic encryption lets you protect only a special type of custom text field, which you create for that purpose.

Feature	Classic Encryption	Platform Encryption
Pricing	Included in base user license	Additional fee applies
Encryption at Rest	✓	✓
Native Solution (No Hardware or Software Required)	✓	✓
Encryption Algorithm	128-bit Advanced Encryption Standard (AES)	256-bit Advanced Encryption Standard (AES)
HSM-based Key Derivation		✓
Manage Encryption Keys Permission		✓
Generate, Export, Import, and Destroy Keys	✓	✓

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Feature	Classic Encryption	Platform Encryption
PCI-DSS L1 Compliance	✓	✓
Masking	✓	
Mask Types and Characters	✓	
View Encrypted Data Permission Required to Read Encrypted Field Values	✓	
Encrypted Standard Fields		✓
Encrypted Attachments, Files, and Content		✓
Encrypted Custom Fields	Dedicated custom field type, limited to 175 characters	✓
Encrypt Existing Fields for Supported Custom Field Types		✓
Search (UI, Partial Search, Lookups, Certain SOSL Queries)		✓
API Access	✓	✓
Available in Workflow Rules and Workflow Field Updates		✓
Available in Approval Process Entry Criteria and Approval Step Criteria		✓

Behind the Scenes: The Shield Platform Encryption Process

When users submit data, the application server looks for the org-specific data encryption key in its cache. If it isn't there, the application server gets the encrypted tenant secret from the database and asks the key derivation server to derive the key. The Shield Platform Encryption service then encrypts the data on the application server. If customers opt out of key derivation or use the Cache-Only Key Service, the encryption service applies the customer-supplied data encryption key directly to customer data.

Important: Where possible, we changed noninclusive terms to align with our company value of Equality. We maintained certain terms to avoid any effect on customer implementations.

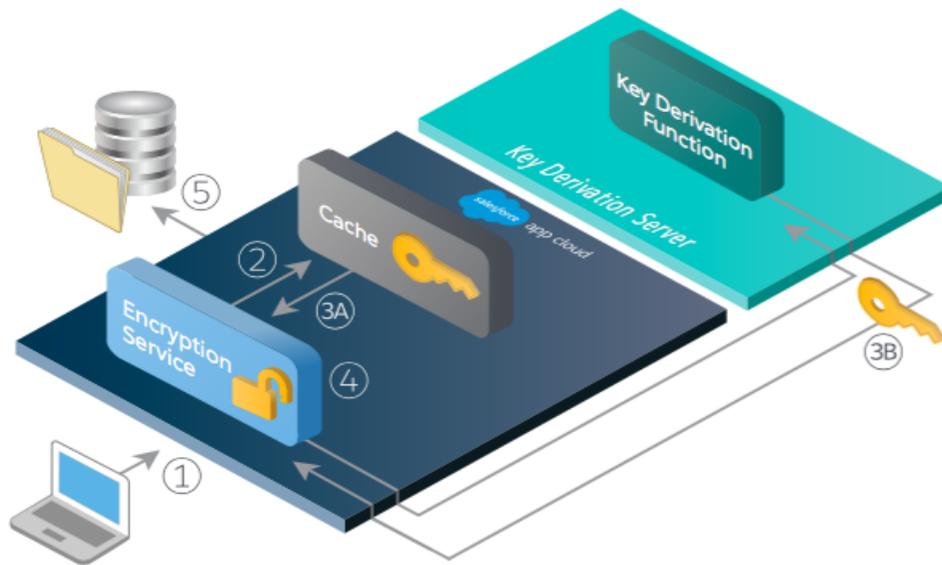
Salesforce securely generates the master and tenant secrets by using Hardware Security Modules (HSMs). The unique key is derived by using PBKDF2, a Key Derivation Function (KDF), with the master and tenant secrets as inputs.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Shield Platform Encryption Process Flow



1. When a Salesforce user saves encrypted data, the runtime engine determines from metadata whether to encrypt the field, file, or attachment before storing it in the database.
2. If so, the encryption service checks for the matching data encryption key in cached memory.
3. The encryption service determines whether the key exists.
 - a. If so, the encryption service retrieves the key.
 - b. If not, the service sends a derivation request to a key derivation server and returns it to the encryption service running on the Salesforce Platform.
4. After retrieving or deriving the key, the encryption service generates a random initialization vector (IV) and encrypts the data using 256-bit AES encryption.
5. The ciphertext is saved in the database or file storage. The IV and corresponding ID of the tenant secret used to derive the data encryption key are saved in the database.

Salesforce generates a new master secret at the start of each release.

Behind the Scenes: The Search Index Encryption Process

The Salesforce search engine is built on the open-source enterprise search platform software Apache Solr. The search index, which stores tokens of record data with links back to the original records stored in the database, is housed within Solr. Partitions divide the search index into segments to allow Salesforce to scale operations. Apache Lucene is used for its core library.

Using Shield Platform Encryption's HSM-based key derivation architecture, metadata, and configurations, Search Index Encryption runs when Shield Platform Encryption is in use. The solution applies strong encryption on an org-specific search index (.fdt, .tim, and .tip file types) using an org-specific AES-256 bit encryption key. The search index is encrypted at the search index segment level, and all search index operations require index blocks to be encrypted in memory.

The only way to access the search index or the key cache is through programmatic APIs.

A Salesforce security administrator can enable Search Index Encryption from Setup. The administrator first creates a tenant secret of the Search Index type, then enables Encryption for Search Indexes. The admin configures their encryption policy by selecting fields and files to encrypt. An org-specific HSM-derived key is derived from the tenant secret on demand. The key material is passed to the search engine's cache on a secure channel.

The process when a user creates or edits records:

1. The core application determines if the search index segment should be encrypted or not based on metadata.
2. If the search index segment should be encrypted, the encryption service checks for the matching search encryption key ID in the cached memory.
3. The encryption service determines if the key exists in the cache.
 - a. If the key exists in the cache, the encryption service uses the key for encryption.
 - b. Otherwise, the service sends a request to the core application, which in turn sends an authenticated derivation request to a key derivation server and returns the key to the core application server.
4. After retrieving the key, the encryption service generates a random initialization vector (IV) and encrypts the data using NSS or JCE's AES-256 implementation.
5. The key ID (identifier of the key being used to encrypt the index segment) and IV are saved in the search index.

The process is similar when a user searches for encrypted data:

1. When a user searches for a term, the term is passed to the search index, along with which Salesforce objects to search.
2. When the search index executes the search, the encryption service opens the relevant segment of the search index in memory and reads the key ID and IV.
3. Steps 3 through 5 of the process when a user creates or edits records are repeated.
4. The search index processes the search and returns the results to the user seamlessly.

If Salesforce admins disable encryption on a field, all index segments that were encrypted are unencrypted and the key ID is set to null. This process can take up to seven days.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

How Does Shield Platform Encryption Work in a Sandbox?

Refreshing a sandbox from a production org creates an exact copy of the production org. If Shield Platform Encryption is enabled on the production org, all encryption settings are copied, including tenant secrets created in production.

Once a sandbox is refreshed, tenant secret changes are confined to your current org. This means that when you rotate or destroy a tenant secret on sandbox, it doesn't affect the production org.

As a best practice, rotate tenant secrets on sandboxes after a refresh. Rotation ensures that production and sandbox use different tenant secrets. Destroying tenant secrets on a sandbox renders encrypted data unusable in cases of partial or full copies.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

Why Bring Your Own Key?

Shield Platform Encryption's Bring Your Own Key (BYOK) feature gives you an extra layer of protection if there is unauthorized access to critical data. It could also help you meet the regulatory requirements that come with handling financial data, such as credit card numbers; health data, such as patient care records or insurance information; or other kinds of private data, such as social security numbers, addresses, and phone numbers. After you've set up your key material, you can use Shield Platform Encryption as you normally would to encrypt data at rest in your Salesforce org.

 **Important:** Where possible, we changed noninclusive terms to align with our company value of Equality. We maintained certain terms to avoid any effect on customer implementations.

Shield Platform Encryption enables Salesforce administrators to manage the lifecycle of their data encryption keys while protecting these keys from unauthorized access. By controlling the lifecycle of your organization's tenant secrets, you control the lifecycle of the data encryption keys derived from them. Alternatively, you can opt out of key derivation altogether and upload a final data encryption key.

Data encryption keys aren't stored in Salesforce. Instead, they're derived from the master secret and tenant secret on demand whenever a key is needed to encrypt or decrypt customer data. The master secret is generated once per release for everyone by a hardware security module (HSM). The tenant secret is unique to your org, and you control when it's generated, activated, revoked, or destroyed.

You have four options for setting up your key material.

- Use the Shield Key Management Service (KMS) to generate your org-specific tenant secret for you.
- Use the infrastructure of your choice, such as an on-premises HSM, to generate and manage your tenant secret outside of Salesforce. Then upload that tenant secret to the Salesforce KMS. This option is popularly known as "Bring Your Own Key," although the element you're really bringing is the tenant secret from which the key is derived.
- Opt out of the Shield KMS key derivation process with the Bring Your Own Key service. Use the infrastructure of your choice to create a data encryption key instead of a tenant secret. Then upload this data encryption key to the Shield KMS. When you opt out of derivation on a key-by-key basis, the Shield KMS bypasses the derivation process and uses this key material as your final data encryption key. You can rotate customer-supplied data encryption keys just like you would rotate a customer-supplied tenant secret.

EDITIONS

Available as an add-on subscription in: **Enterprise, Performance, and Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

EDITIONS

Available as an add-on subscription in: **Enterprise, Performance, and Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

- Generate and store your key material outside of Salesforce using a key service of your choice, and use the Salesforce Cache-Only Key Service to fetch your key material on demand. Your key service transmits your key material over a secure channel that you configure. It's then encrypted and stored in the cache for immediate encrypt and decrypt operations.

Why Isn't My Encrypted Data Masked?

If the Shield Platform Encryption service isn't available, data is masked in some types of encrypted fields. This is to help you troubleshoot encryption key issues, not to control user access to data. If you have data that you don't want some users to see, revisit those users' field-level security settings, record access settings, and object permissions.

Encryption prevents outsiders from using your Salesforce data even if they manage to get it. It is not a way to hide data from authenticated users. User permissions are the only way to control data visibility for authenticated users. Encryption at rest is about logins, not permissions.

With Shield Platform Encryption, if a user is authorized to see a given set of data, that user sees that data whether it's encrypted or not.

- Authentication means that making sure only legitimate users can get into your system. For example, a company's Salesforce org is only for use by active employees of that company. Anyone who is not an employee is not authenticated; that is, they are barred from logging in. If they do somehow get their hands on the data, it's useless to them because it is encrypted.
- Authorization defines which data or features an authenticated user can use. For example, a sales associate can see and use data in the Leads object, but can't see the regional forecasts, which are intended for sales managers. Both the associate and the manager are properly logged in (authenticated), but their permissions (authorization) are different. That the data is encrypted doesn't make any difference to them.

In general, data can be masked but not encrypted, or encrypted but not masked. For example, regulators often require that only the last four digits of a credit card number be visible to users. Applications typically mask the rest of the number, meaning they replace the digits with asterisks on the user's screen. Without encryption, you can still read the digits that are masked if you can get to the database where they are stored.

Masking might not be enough for your credit card numbers. You may or may not want to encrypt them in the database as well. (You probably should.) If you do, authenticated users will still see the same masked values.

In this way, masking and encryption are different solutions for different problems. You mask data to hide it from users who are authenticated but not authorized to see that data. You encrypt data to prevent someone from stealing the data. (Or, more precisely, to make the data useless if someone does steal it.)

The following table shows the fields that use masking. All others don't.

Field Type	Mask	What It Means
Email, Phone, Text, Text Area, Text Area (Long), URL	?????	This field is encrypted, and the encryption key has been destroyed.
	!!!!	This service is unavailable right now. For help accessing this service, contact Salesforce.
Custom Date	08/08/1888	This field is encrypted, and the encryption key has been destroyed.
	01/01/1777	This service is unavailable right now. For help accessing this service, contact Salesforce.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Field Type	Mask	What It Means
Custom Date/Time	08/08/1888 12:00 PM	This field is encrypted, and the encryption key has been destroyed.
	01/01/1777 12:00 PM	This service is unavailable right now. For help accessing this service, contact Salesforce.

You can't enter these masking characters into an encrypted field. For example, if a Date field is encrypted and you enter 07/07/1777, you must enter a different value before it can be saved.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

Shield Platform Encryption in Hyperforce

Shield Platform Encryption operates in parallel with volume-level encryption. By default, Hyperforce provides volume-level encryption for data at rest. Volume-level encryption protects all the data on a disk with one encryption key, which Salesforce owns and manages. With Shield Platform Encryption, you can encrypt your data in Hyperforce with unique keys that you control and manage.

Shield Platform Encryption features work in Hyperforce just like they do in implementations running on Salesforce's first-party infrastructure. You can generate a unique key with Salesforce, or bring your own customer-supplied key, and rotate, export, and delete key material on demand. You can also encrypt files and attachments and data in CRM Analytics, Chatter, search indexes, and the event bus. And you can gather statistics about how much of your data is encrypted and, of that data, how much of it's encrypted by active key material. This extra layer of security and control can help you meet your auditing, regulatory, contractual, and compliance requirements.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

How Do I Deploy Shield Platform Encryption?

When you deploy Shield Platform Encryption to your org with a tool such as Salesforce Extensions for Visual Studio Code, Migration Tool, or Postman, the Encrypted field attribute persists. However, if you deploy to orgs with different encryption settings, the effect depends on whether Shield Platform Encryption is enabled in the target org.

Regardless of how you deploy, Salesforce automatically checks to see if the implementation violates Shield Platform Encryption guidelines.

Source Organization	Target Organization	Result
Shield Platform Encryption enabled	Shield Platform Encryption enabled	The source Encrypted field attribute indicates enablement.
Shield Platform Encryption enabled	Shield Platform Encryption not enabled	The Encrypted field attribute is ignored.
Shield Platform Encryption not enabled	Shield Platform Encryption enabled	The target Encrypted field attribute indicates enablement.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

SEE ALSO:

[Fix Compatibility Problems](#)

[How Does Shield Platform Encryption Work in a Sandbox?](#)

Set Up Your Encryption Policy

An encryption policy is your plan for encrypting data with Shield Platform Encryption. You can choose how you want to implement it. For example, you can encrypt individual fields and apply different encryption schemes to those fields. Or you can choose to encrypt other data elements such as files and attachments, data in Chatter, or search indexes. Remember that encryption is not the same thing as field-level security or object-level security. Put those controls in place before you implement your encryption policy.

To provide Shield Platform Encryption for your org, contact your Salesforce account executive. They'll help you provision the correct license so you can create key material and start encrypting data.

 **Warning:** Salesforce recommends testing Shield Platform Encryption in a sandbox org to confirm that your reports, dashboards, processes, and other operations work correctly.

1. [Which User Permissions Does Shield Platform Encryption Require?](#)

Assign permissions to your users according to their roles regarding encryption and key management. Some users need permission to select data for encryption, while other users require combinations of permissions to work with certificates or key material. Enable these permissions for user profiles just like you do for any other user permission.

2. [Generate a Tenant Secret with Salesforce](#)

Salesforce makes it easy to generate a unique tenant secret from the Setup menu.

3. [Manage Tenant Secrets by Type](#)

With tenant secret types, you can specify which kind of data you want to encrypt with a Shield Platform Encryption tenant secret. You can apply different key rotation cycles or key destruction policies to tenant secrets that encrypt different kinds of data. You can apply a tenant secret to search index files and other data stored in Salesforce.

4. [Encrypt New Data in Standard Fields](#)

You can encrypt standard fields on standard objects at rest with Shield Platform Encryption. For the best results, encrypt the least number of fields possible.

5. [Encrypt Fields on Custom Objects and Custom Fields](#)

You can encrypt standard fields on custom objects, and custom fields on both standard and custom objects. Shield Platform Encryption also supports custom fields in installed managed packages. Apply encryption to custom fields from the management settings for each object. For best results, encrypt the least number of fields possible. When you add encryption to a field, all new data in that field is encrypted.

6. [Encrypt New Files and Attachments](#)

For another layer of data protection, encrypt files and attachments. If Shield Platform Encryption is on, the body of each file or attachment is encrypted when it's uploaded.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

7. [Encrypt Data in Chatter](#)

Enabling Shield Platform Encryption for Chatter adds an extra layer of security to the information that users share in Chatter. You can encrypt data at rest in feed posts and comments, questions and answers, link names and URLs, poll questions and choices, and content from your custom rich publisher apps.

8. [Encrypt Search Index Files](#)

Sometimes you must search for personally identifiable information (PII) or data that's encrypted in the database. When you search your org, the results are stored in search index files. You can encrypt these search index files with Shield Platform Encryption, adding another layer of security to your data.

9. [Encrypt CRM Analytics Data](#)

To get started with CRM Analytics Encryption, generate a tenant secret with Shield Platform Encryption. After you generate a CRM Analytics tenant secret, CRM Analytics Encryption uses the Shield Platform Encryption key management architecture to encrypt your CRM Analytics data.

10. [Encrypt Event Bus Data](#)

To enable encryption of change data capture or platform event messages at rest, generate an event bus tenant secret and then enable encryption.

11. [Fix Compatibility Problems](#)

When you select fields or files to encrypt with Shield Platform Encryption, Salesforce automatically checks for potential side effects. The validation service then warns you if any existing settings may pose a risk to data access or your normal use of Salesforce. You have some options for how to clear up these problems.

12. [Disable Encryption on Fields](#)

You can disable Shield Platform Encryption for fields, files, or both. You can turn field encryption on or off individually, but file encryption is all or nothing.

SEE ALSO:

[Strengthen Your Data's Security with Shield Platform Encryption](#)

Which User Permissions Does Shield Platform Encryption Require?

Assign permissions to your users according to their roles regarding encryption and key management. Some users need permission to select data for encryption, while other users require combinations of permissions to work with certificates or key material. Enable these permissions for user profiles just like you do for any other user permission.

	Manage Encryption Keys	Customize Application	View Setup and Configuration	Manage Certificates
View Platform Encryption Setup pages		✓	✓	
Generate, destroy, export, import, and upload tenant secrets and customer-supplied key material	✓			
Query the TenantSecret object via the API	✓			
Edit, upload, and download HSM-protected certificates with the	✓	✓		✓

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

	Manage Encryption Keys	Customize Application	View Setup and Configuration	Manage Certificates
Shield Platform Encryption Bring Your Own Key service				
Enable features on the Encryption Settings page	✓	✓		

The Customize Application and Manage Certificates permissions are automatically enabled for users with the System Administrator profile.

Restrict Access to Encryption Policy Settings

You can require admins to also have the Manage Encryption Keys permission to complete encryption policy tasks. These tasks include changing the encryption scheme on fields, enabling and disabling encryption on fields, files, and attachments, and other data elements.

To opt in to this feature, you need the Manage Encryption Keys permission. Then opt in from the Encryption Settings page.

1. From Setup, in the Quick Find box, enter *Encryption Settings*, and then select **Encryption Settings**.
2. In the Advanced Encryption Settings section, turn on **Restrict Access to Encryption Policy Settings**.

You can also enable Restrict Access to Encryption Policy Settings programmatically. For more information, see [PlatformEncryptionSettings](#) in the *Metadata API Developer Guide*.

This restriction applies to actions taken through the API or from Setup pages, such as the Encryption Policy page or the Object Manager.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

SEE ALSO:

[User Permissions](#)

[Metadata API Developer Guide: EncryptionKeySettings](#)

[Metadata API Developer Guide: PlatformEncryptionSettings](#)

Generate a Tenant Secret with Salesforce

Salesforce makes it easy to generate a unique tenant secret from the Setup menu.

Only authorized users can generate tenant secrets from the Platform Encryption page. Ask your Salesforce admin to assign you the Manage Encryption Keys permission.

1. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Key Management**.
2. In the Key Management Table, select a key type.
3. Click **Generate Tenant Secret**.

How often you can generate a tenant secret depends on the tenant secret type. You can generate tenant secrets for the Fields and Files (Probabilistic) type once every 24 hours in production orgs, and once every 4 hours in Sandbox orgs. You can generate tenant secrets for the Search Index type once every 7 days.

 **Note:** You can have up to 50 active and archived tenant secrets of each type. For example, you can have one active and 49 archived Fields and Files (Probabilistic) tenant secrets, and the same number of Analytics tenant secrets. This limit includes Salesforce-generated and customer-supplied key material.

If you run into this limit, destroy an existing key before reactivating, rearchiving, or creating a callout to another one. Before destroying a key, synchronize the data it encrypts with an active key.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

SEE ALSO:

[API Guide: TenantSecret](#)

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:

- **Manage Encryption Keys**

Manage Tenant Secrets by Type

With tenant secret types, you can specify which kind of data you want to encrypt with a Shield Platform Encryption tenant secret. You can apply different key rotation cycles or key destruction policies to tenant secrets that encrypt different kinds of data. You can apply a tenant secret to search index files and other data stored in Salesforce.

Tenant secrets are categorized according to the kind of data they encrypt.

Fields and Files (Probabilistic)

Encrypts data using the probabilistic encryption scheme, including data in fields, attachments, and files other than search index files.

Field (Deterministic)

Encrypts field data using the deterministic encryption scheme.

Search Index

Encrypts search index files.

Analytics

Encrypts CRM Analytics data.

Event Bus

Encrypts event messages that are stored temporarily in the event bus. For change data capture events, this secret encrypts data changes and the corresponding event that contains them. For platform events, this secret encrypts the event message including event field data.

Note:

- Tenant secrets that were generated or uploaded before Spring '17 are categorized as the Fields and Files (Probabilistic) type.
- You can have up to 50 active and archived tenant secrets of each type. For example, you can have one active and 49 archived Fields and Files (Probabilistic) tenant secrets, and the same number of Analytics tenant secrets. This limit includes Salesforce-generated and customer-supplied key material.

If you run into this limit, destroy an existing key before reactivating, rearchiving, or creating a callout to another one. Before destroying a key, synchronize the data it encrypts with an active key.

1. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Key Management**.
2. In the Key Management Table, select a key type.

The Key Management Table displays all tenant secrets of each data type. If you generate or upload a tenant secret while viewing tenant secrets of a particular type, it becomes the active tenant secret for that data.

Note: This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

SEE ALSO:

[API Guide: TenantSecret](#)

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:

- Manage Certificates
AND
Manage Encryption Keys

Encrypt New Data in Standard Fields

You can encrypt standard fields on standard objects at rest with Shield Platform Encryption. For the best results, encrypt the least number of fields possible.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

Depending on the size of your org, enabling a standard field for encryption can take a few minutes.

1. Make sure that your org has an active encryption key. If you're not sure, check with your administrator.
2. From Setup, in the Quick Find box, enter *Encryption Settings*, and then select **Encryption Settings**.
3. In the Advanced Encryption Settings section, click **Select Fields**.
4. Click **Edit**.
5. Select the fields that you want to encrypt.
All new data entered in this field is encrypted. By default, data is encrypted using a probabilistic encryption scheme. To apply deterministic encryption to your data, select **Deterministic** from the Encryption Scheme list. For more information, see "How Deterministic Encryption Supports Filtering" in Salesforce Help.
6. Save your work.

The automatic Platform Encryption validation service checks for settings in your org that can block encryption. You receive an email with suggestions for fixing incompatible settings.

Field values are automatically encrypted only in records created or updated after you've enabled encryption. Synchronize existing data with your active key material on the Encryption Statistics and Data Sync page.

 **Note:** To encrypt standard fields on custom objects, such as Custom Object Name, see [Encrypt Fields on Custom Objects and Custom Fields](#).

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:

- View Setup and Configuration

To encrypt fields:

- Customize Application

Encrypt Fields on Custom Objects and Custom Fields

You can encrypt standard fields on custom objects, and custom fields on both standard and custom objects. Shield Platform Encryption also supports custom fields in installed managed packages. Apply encryption to custom fields from the management settings for each object. For best results, encrypt the least number of fields possible. When you add encryption to a field, all new data in that field is encrypted.

[Encrypt New Data in Custom Fields in Salesforce Classic](#)

Apply Shield Platform Encryption to new custom fields in Salesforce Classic, or add encryption to new data entered in an existing custom field.

[Encrypt New Data in Custom Fields in Lightning Experience](#)

Apply Shield Platform Encryption to new custom fields in Lightning Experience, or add encryption to new data entered in an existing custom field.

[Encrypt Custom Fields in Installed Managed Packages](#)

If an installed managed package supports Shield Platform Encryption, you can encrypt custom fields in that package. Turn on encryption for custom fields in installed managed packages from the Encryption Settings page, and then apply encryption to custom fields in your installed managed package.

Encrypt New Data in Custom Fields in Salesforce Classic

Apply Shield Platform Encryption to new custom fields in Salesforce Classic, or add encryption to new data entered in an existing custom field.

To apply deterministic encryption to custom fields, first turn on deterministic encryption from the Encryption Settings page in Setup.

1. From the management settings for the object, go to **Fields**.
2. In the Custom Fields & Relationships section, create a field or edit an existing one.
3. Select **Encrypted**.
All new data entered in this field is encrypted. By default, data is encrypted using a probabilistic encryption scheme. To apply deterministic encryption to your data, select a deterministic option listed under Encrypted.
4. Save your work.

The automatic Shield Platform Encryption validation service checks for settings in your org that can block encryption. You receive an email with suggestions for fixing incompatible settings.

Field values are automatically encrypted only in records created or updated after you've enabled encryption. Synchronize your existing data with your active key material from the Encryption Statistics and Data Sync page.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:

- View Setup and Configuration

To encrypt fields:

- Customize Application

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:

- View Setup and Configuration

To encrypt fields:

- Customize Application

Encrypt New Data in Custom Fields in Lightning Experience

Apply Shield Platform Encryption to new custom fields in Lightning Experience, or add encryption to new data entered in an existing custom field.

To apply deterministic encryption to custom fields, first turn on deterministic encryption from the Encryption Settings page in Setup.

1. From Setup, select **Object Manager**, and then select your object.
2. Click **Fields & Relationships**.
3. When you create or edit a custom field, select **Encrypted**.
All new data entered in this field is encrypted. By default, data is encrypted using a probabilistic encryption scheme. To apply deterministic encryption to your data, select a deterministic option listed under Encrypted.
4. Save your work.

The automatic Platform Encryption validation service checks for settings in your org that can block encryption. You receive an email with suggestions for fixing incompatible settings.

Field values are automatically encrypted only in records created or updated after you've enabled encryption. Synchronize existing data with your active key material from the Encryption Statistics and Data Sync page.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

Encrypt Custom Fields in Installed Managed Packages

If an installed managed package supports Shield Platform Encryption, you can encrypt custom fields in that package. Turn on encryption for custom fields in installed managed packages from the Encryption Settings page, and then apply encryption to custom fields in your installed managed package.

1. From Setup, in the Quick Find box, enter *Encryption Settings*, and then select **Encryption Settings**.
2. In the Advanced Encryption Settings section, turn on **Encrypt Custom Fields in Managed Packages**.

You can also enable encryption for managed packages programmatically. For more information, see [PlatformEncryptionSettings](#) in the *Metadata API Developer Guide*.

From now on, if an installed managed package supports encryption, you can encrypt custom fields in that package. Don't know if your application supports encrypted fields? Look for the Designed to Work With Salesforce Shield marker in your application's AppExchange listing.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:

- View Setup and Configuration

To encrypt fields:

- Customize Application

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To enable features on the Encryption Settings page:

- Customize Application



If you don't see this marker, talk to your app vendor.

 **Note:** If Salesforce enabled this feature for you before Spring '19, opt in again on the Encryption Settings page. If you don't opt in, you can't enable or disable encryption on those fields. However, your encrypted custom fields in installed managed packages remain encrypted.

Encrypt New Files and Attachments

For another layer of data protection, encrypt files and attachments. If Shield Platform Encryption is on, the body of each file or attachment is encrypted when it's uploaded.

 **Note:** Before you begin, make sure that your org has an active encryption key. If you're not sure, check with your Salesforce admin.

1. From Setup, in the Quick Find box, enter *Encryption Settings*, and then select **Encryption Settings**.
2. In the Encryption Policy section, turn on **Encrypt Files and Attachments**.

 **Important:** Users with access to the file can work normally with it regardless of their encryption-specific permissions. Users who are logged in to your org and have read access can search and view the body content.

Users can continue to upload files and attachments per the usual file size limits. Expansion of file sizes caused by encryption doesn't count against these limits.

Turning on file and attachment encryption affects new files and attachments. It doesn't automatically encrypt files and attachments that are already in Salesforce. Apply your active key material to existing data with on the Encryption Statistics and Data Sync page.

To check whether a file or attachment is encrypted, look for the encryption indicator on the detail page of the file or attachment. You can also query the `isEncrypted` field on the ContentVersion object (for files) or on the Attachment object (for attachments).

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

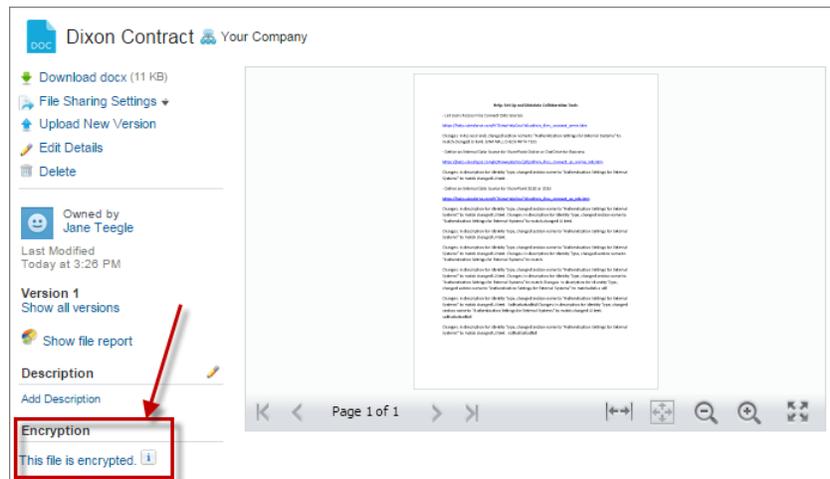
To view setup:

- View Setup and Configuration

To encrypt files:

- Customize Application

Here's What It Looks Like When a File Is Encrypted



Note: The encryption indicator is only available in Salesforce Classic.

Encrypt Data in Chatter

Enabling Shield Platform Encryption for Chatter adds an extra layer of security to the information that users share in Chatter. You can encrypt data at rest in feed posts and comments, questions and answers, link names and URLs, poll questions and choices, and content from your custom rich publisher apps.

We recommend that you test Encryption for Chatter in a dedicated Sandbox environment before enabling it in production.

Unlike encryption for custom and standard fields, enabling encryption for Chatter encrypts all eligible Chatter fields.

1. Make sure that your org has an active encryption key. If you're not sure, check with your administrator.
2. From Setup, in the Quick Find box, enter *Encryption Settings*, and then select **Encryption Settings**.
3. In the Encryption Policy section, turn on **Encrypt Chatter**.

The automatic Shield Platform Encryption validation service checks for settings that could block encryption. If the service finds potential problems, it sends you an email with suggestions for fixing the problems.

After you activate encryption for Chatter, new data that you enter into Chatter gets encrypted. To encrypt historic Chatter data, contact Salesforce Customer Support to request the background encryption service.

When you edit or update an encrypted Chatter field, the field's revision history is also encrypted. For example, if you update a post, the old version of the post remains encrypted.

If you enabled Encryption for Chatter in Spring '17 and you want to access the most up-to-date features, deselect **Encrypt Chatter** and then reselect **Encrypt Chatter**.



Note: This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:

- View Setup and Configuration

To encrypt fields:

- Customize Application

Encrypt Search Index Files

Sometimes you must search for personally identifiable information (PII) or data that's encrypted in the database. When you search your org, the results are stored in search index files. You can encrypt these search index files with Shield Platform Encryption, adding another layer of security to your data.

1. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Key Management**.
2. In the Key Management Table, select **Search Index**.
3. Select **Generate Tenant Secret**.
This new tenant secret encrypts only the data stored in search index files.
4. From Setup, in the Quick Find box, enter *Encryption Settings*, and then select **Encryption Settings**.
5. In the Encryption Policy section, turn on **Encrypt Search Indexes**.
Your search indexes are now encrypted with the active Search Index tenant secret.

SEE ALSO:

[Behind the Scenes: The Search Index Encryption Process](#)
[Generate a Tenant Secret with Salesforce](#)

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:

- View Setup and Configuration

To enable encryption key (tenant secret) management:

- Manage Profiles and Permission Sets

Encrypt CRM Analytics Data

To get started with CRM Analytics Encryption, generate a tenant secret with Shield Platform Encryption. After you generate a CRM Analytics tenant secret, CRM Analytics Encryption uses the Shield Platform Encryption key management architecture to encrypt your CRM Analytics data.

You must be approved by the CRM Analytics Encryption Product Manager to use CRM Analytics Encryption. To request access, file a case with Salesforce Customer Support.

To learn about CRM Analytics' key management architecture, read [Strengthen Your Data's Security with Shield Platform Encryption](#).

1. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Key Management**.
2. In the Key Management Table, select **Analytics**.
3. Generate a tenant secret or upload key material.
4. From Setup, in the Quick Find box, enter *Encryption Settings*, and then select **Encryption Settings**.
5. In the Encryption Policy section, select **Encrypt CRM Analytics**.
New datasets in CRM Analytics are now encrypted.

 **Note:** Data that was in CRM Analytics before encryption was enabled isn't encrypted. If preexisting data is imported from Salesforce objects through the dataflow, the data becomes encrypted on the next dataflow run. Other preexisting data, such as CSV data, must be reimported to become encrypted. Although preexisting data isn't encrypted, it's still accessible and fully functional in its unencrypted state when encryption is enabled.

SEE ALSO:

[Generate a Tenant Secret with Salesforce](#)

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing CRM Analytics Platform and either Salesforce Shield or the Platform Encryption add-on.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:

- View Setup and Configuration

To manage key material:

- Manage Encryption Keys

Encrypt Event Bus Data

To enable encryption of change data capture or platform event messages at rest, generate an event bus tenant secret and then enable encryption.

These steps enable encryption for change data capture and platform events.

1. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Key Management**.
2. In the Key Management Table, select **Event Bus**.
3. Click **Generate Tenant Secret**, or to upload a customer-supplied tenant secret, click **Bring Your Own Key**, and upload your key.
4. From Setup, in the Quick Find box, enter *Encryption Settings*, and then select **Encryption Settings**.
5. In the Encryption Policy section, turn on **Encrypt Change Data Capture Events and Platform Events**.



Warning: If you don't enable Shield Platform Encryption for change data capture events and platform events, events are stored in clear text in the event bus.

SEE ALSO:

[Change Data Capture Developer Guide](#)

[Platform Events Developer Guide](#)

Fix Compatibility Problems

When you select fields or files to encrypt with Shield Platform Encryption, Salesforce automatically checks for potential side effects. The validation service then warns you if any existing settings may pose a risk to data access or your normal use of Salesforce. You have some options for how to clear up these problems.

If your results include error messages, you're probably running into one or more of these limitations:

Portals

You can't encrypt standard fields, because a legacy customer or partner portal (created before 2013) is enabled in your organization. To deactivate a legacy customer portal, go to the Customer Portal Settings page in Setup. To deactivate a legacy partner portal, go to the Partners page in Setup.



Note: Experience Cloud sites aren't related to this issue. They're fully compatible with encryption.

Criteria-Based Sharing Rules

You've selected a field that is used in a filter in a criteria-based sharing rule.

SOQL/SOSL queries

You've selected a field that's used in an aggregate function in a SOQL query, or in a WHERE, GROUP BY, or ORDER BY clause.

Formula fields

You've selected a field that's referenced by a custom formula field in an unsupported way. Formulas can use BLANKVALUE, CASE, HYPERLINK, IF, IMAGE, ISBLANK, ISNULL, NULLVALUE, and concatenation (&).

Flows and Processes

You've selected a field that's used in one of these contexts.

EDITIONS

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions. Requires purchasing either Salesforce Shield or the Platform Encryption add-on.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:

- View Setup and Configuration

To manage key material:

- Manage Encryption Keys

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

- To filter data in a flow
- To sort data in a flow
- To filter data in a process
- To filter data in a record choice set
- To sort data in a record choice set

 **Note:** By default, your results only list the first 250 errors per element. You can increase the number of errors listed in your results to 5000. Contact Salesforce for help.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

Disable Encryption on Fields

You can disable Shield Platform Encryption for fields, files, or both. You can turn field encryption on or off individually, but file encryption is all or nothing.

When you turn off Shield Platform Encryption for a field, most encrypted data is automatically mass-decrypted. The decryption starts automatically after you disable encryption for specific fields and save your changes. When data is decrypted, any functionality that was limited or unavailable when the data was encrypted is also restored. Salesforce notifies you by email when the decryption process is complete.

 **Note:** Automatic decryption takes longer when you disable encryption on fields encrypted with a key that's been destroyed. Salesforce notifies you by email when the process finishes.

Long text area and rich text area field types can't be automatically decrypted. If you decrypt data encrypted with a destroyed key, that data can't be mass-decrypted.

 **Note:** If you disable Shield Platform Encryption and can't access data in fields that were previously encrypted, contact Salesforce for help.

1. From Setup, in the Quick Find box, enter *Encryption Settings*, and then select **Encryption Settings**.
2. In the Advanced Encryption Settings section, click **Select Fields**.
3. Click **Edit**.
4. Deselect the fields that you want to stop encrypting and save your work. Users can see data in these fields.
5. To disable encryption for files and attachments, Chatter, or other data categories, turn off those features from the Encryption Settings page and save your work.

After your data is decrypted, functionality that Shield Platform Encryption limited or changed is restored.

SEE ALSO:

[Set Up Your Encryption Policy](#)

Filter Encrypted Data with Deterministic Encryption

You can filter data that's protected with Shield Platform Encryption using deterministic encryption. Your users can filter records in reports and list views, even when the underlying fields are encrypted. You can apply case-sensitive deterministic encryption or exact-match case-insensitive deterministic encryption to data on a field-by-field basis.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:

- View Setup and Configuration

To disable encryption:

- Customize Application

Deterministic encryption supports WHERE clauses in SOQL queries and is compatible with unique and external ID fields. It also supports single-column indexes and single and double-column unique indexes. Deterministic encryption key types use the Advanced Encryption Standard (AES) with 256-bit keys with CBC mode and a static initialization vector (IV).

[How Deterministic Encryption Supports Filtering](#)

By default, Shield Platform Encryption uses a probabilistic encryption scheme to encrypt data. Each bit of data is turned into a fully random ciphertext string every time it's encrypted. Encryption doesn't generally impact users who are authorized to view the data. The exceptions are when logic is executed in the database or when encrypted values are compared to a string or to each other. In these cases, because the data has been turned into random, patternless strings, filtering isn't possible. For example, you might run a SOQL query in custom Apex code against the Contact object, where LastName = 'Smith'. If the LastName field is encrypted with probabilistic encryption, you can't run the query. Deterministic encryption addresses this problem.

[Encrypt Data with the Deterministic Encryption Scheme](#)

Generate key material specific to data encrypted with deterministic encryption schemes. You can apply either case-sensitive deterministic encryption or case-insensitive deterministic encryption schemes to your data, depending on the kind of filtering you want to perform. When you apply a deterministic encryption scheme to a field or change between deterministic encryption schemes, synchronize your data. Syncing data makes sure that your filters and queries produce accurate results.

SEE ALSO:

[Strengthen Your Data's Security with Shield Platform Encryption](#)

How Deterministic Encryption Supports Filtering

By default, Shield Platform Encryption uses a probabilistic encryption scheme to encrypt data. Each bit of data is turned into a fully random ciphertext string every time it's encrypted. Encryption doesn't generally impact users who are authorized to view the data. The exceptions are when logic is executed in the database or when encrypted values are compared to a string or to each other. In these cases, because the data has been turned into random, patternless strings, filtering isn't possible. For example, you might run a SOQL query in custom Apex code against the Contact object, where LastName = 'Smith'. If the LastName field is encrypted with probabilistic encryption, you can't run the query. Deterministic encryption addresses this problem.

To be able to use filters when data is encrypted, we have to allow some patterns in our data. Deterministic encryption uses a static initialization vector (IV) so that encrypted data can be matched to a particular field value. The system can't read a piece of data that's encrypted, but it does know how to retrieve the ciphertext that stands for that piece of data thanks to the static IV. The IV is unique for a given field in a given org and can only be decrypted with your org-specific encryption key.

We evaluate the relative strengths and weaknesses of cryptographic approaches based on the types of attacks that can be launched against a particular algorithm. We also consider the length of time that it could take for the attack to succeed. For example, it is commonly said that a brute-force attack against an AES 256-bit key would take a billion billion years given current computing capabilities. Nevertheless, it is common practice to rotate keys regularly.

Certain kinds of attacks become a bit less far-fetched when you get away from purely random ciphertext. For example, an attacker could conceivably analyze deterministically encrypted ciphertext and determine that the cleartext string Alice always resolves to the ciphertext YjNkY2J1NjU5M2JkNjk4MGJiNWE2NGQ5NzI5MzU1OTcNCg==. Given enough time to eavesdrop, an attacker could defeat encryption by building a dictionary of cleartext values to ciphertext values.

The Salesforce Shield approach is to expose just enough determinism to let bona fide users filter on encrypted data while limiting it enough to ensure that a given plaintext value doesn't universally result in the same ciphertext value across all fields, objects, or orgs. Even if an attacker successfully matched cleartext to encrypted values for one field, the attacker would have to do it all over again for another field, and again for the same field in another object.

In this way, deterministic encryption decreases encryption strength only as minimally necessary to allow filtering.

Deterministic encryption comes in two types: case-sensitive and case-insensitive. With case-sensitive encryption, a SOQL query against the Contact object, where LastName = Jones, returns only Jones, not jones or JONES. Similarly, when the case-sensitive deterministic scheme tests for unicity (uniqueness), each version of "Jones" is unique.

For case-insensitive, a SOQL query against the Lead object, where Company = Acme, returns Acme, acme, or ACME. When the case-insensitive scheme tests for unicity (uniqueness), each version of Acme is considered identical.

 **Important:** Probabilistic encryption is not supported on the email address field for the Contact object. To avoid creating duplicate accounts during self-registration, use deterministic encryption.

Encrypt Data with the Deterministic Encryption Scheme

Generate key material specific to data encrypted with deterministic encryption schemes. You can apply either case-sensitive deterministic encryption or case-insensitive deterministic encryption schemes to your data, depending on the kind of filtering you want to perform. When you apply a deterministic encryption scheme to a field or change between deterministic encryption schemes, synchronize your data. Syncing data makes sure that your filters and queries produce accurate results.

1. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Key Management**.
2. In the Key Management Table, select **Fields and Files (Probabilistic)**.
3. Generate or upload a tenant secret.
4. From Setup, in the Quick Find box, enter *Encryption Settings*, and then select **Encryption Settings**.
5. In the Advanced Encryption Settings section, turn on **Deterministic Encryption**.

You can also enable deterministic encryption programmatically. For more information, see [PlatformEncryptionSettings](#) in the *Metadata API Developer Guide*.

6. From Setup, select **Key Management**.
7. In the Key Management Table, select **Fields (Deterministic)**.
8. Generate a tenant secret.

You can mix and match probabilistic and deterministic encryption, encrypting some fields one way and some fields the other.

9. Enable encryption for each field, and choose a deterministic encryption scheme. How you do that depends on whether it's a standard field or a custom field.
 - For standard fields, from Setup, select **Encryption Policy**, and then select **Encrypt Fields**. For each field that you want to encrypt, select the field name, and then choose either **Deterministic—Case Sensitive** or **Deterministic—Case Insensitive** from the Encryption Scheme list.

USER PERMISSIONS

To generate, destroy, export, import, and upload tenant secrets and customer-supplied key material:

- Manage Encryption Keys

To enable Deterministic Encryption:

- Customize Application

The screenshot shows the 'Account' page in Salesforce. On the left, there is a list of fields with checkboxes: Account Name, Billing Address, Shipping Address, Phone, Fax, Website, and Description. On the right, there is an 'Encryption Scheme' section with a dropdown menu. The dropdown menu is open, showing three options: 'Probabilistic', 'Deterministic - Case Sensitive', and 'Deterministic - Case Insensitive'. The 'Deterministic - Case Insensitive' option is highlighted with a blue bar and an orange border.

- For custom fields, open the Object Manager and edit the field that you want to encrypt. Select **Encrypt the contents of this field**, and select an encryption scheme.

The screenshot shows the 'New Custom Field' page in Salesforce. The page is titled 'Step 2. Enter the details' and 'Step 2 of 4'. There are buttons for 'Previous', 'Next', and 'Cancel'. The 'Field Label' and 'Field Name' are both 'Encrypted_Field'. The 'Description' and 'Help Text' fields are empty. Under the 'Encrypted' section, the checkbox 'Encrypt the contents of this field' is checked. Below it, there are three radio button options: 'Use probabilistic encryption', 'Use case sensitive deterministic encryption', and 'Use case insensitive deterministic encryption'. The 'Use case insensitive deterministic encryption' option is selected and highlighted with an orange border.

You receive an email notifying you when the enablement process finishes.

- Note:** Expect the enablement process to take longer when you apply deterministic encryption to a field with a large number of records. To support filtering, the enablement process also rebuilds field indexes.

- When you apply or remove deterministic encryption to a field, it's possible that existing data in that field doesn't appear in queries or filters. To apply full deterministic functionality to existing data, synchronize all your data with your active key material from the

Encryption Statistics and Data Sync page. For more information, see [Synchronize Your Data Encryption with the Background Encryption Service](#).

SEE ALSO:

[Metadata API Developer Guide: PlatformEncryptionSettings](#)

Key Management and Rotation

Shield Platform Encryption lets you control and rotate the key material used to encrypt your data. You can use Salesforce to generate a tenant secret for you, which is then combined with a per-release master secret to derive a data encryption key. This derived data encryption key is then used in encrypt and decrypt functions. You can also use the Bring Your Own Key (BYOK) service to upload your own key material, or store key material outside of Salesforce and have the Cache-Only Key Service fetch your key material on demand.

 **Important:** Where possible, we changed noninclusive terms to align with our company value of Equality. We maintained certain terms to avoid any effect on customer implementations.

Key management begins with assigning security administrators the appropriate permissions. Assign permissions to people you trust to encrypt data, manage certificates, and work with key material. It's a good idea to monitor these users' key management and encryption activities with the Setup Audit Trail. Authorized developers can generate, rotate, export, destroy, reimport, and upload tenant secrets by coding a call to the TenantSecret object in the Salesforce API.

[Work with Key Material](#)

Shield Platform Encryption lets you generate a unique tenant secret for your org, or generate a tenant secret or key material using your own external resources. In either case, you manage your own key material: You can rotate it, archive it, and designate other users to share responsibility for it.

[Rotate Your Encryption Tenant Secrets](#)

You control the lifecycle of your data encryption keys by controlling the lifecycle of your tenant secrets. Salesforce recommends that you regularly generate or upload new Shield Platform Encryption key material. When you rotate a tenant secret, you replace it with either a Salesforce-generated tenant secret or customer-supplied key material.

[Back Up Your Tenant Secrets](#)

Your Shield Platform Encryption tenant secret is unique to your org and to the specific data to which it applies. Salesforce recommends that you export your tenant secret to ensure continued access to the related data.

[Get Statistics About Your Encryption Coverage](#)

The Encryption Statistics page provides an overview of all data encrypted with Shield Platform Encryption. This information helps you to stay on top of your key rotation and management tasks. You can also use encryption statistics to identify which objects and fields you may want to update after you rotate your key material.

[Synchronize Your Data Encryption with the Background Encryption Service](#)

Periodically, you change your encryption policy. Or you rotate your keys. To get the most protection out of your encryption strategy with Shield Platform Encryption, synchronize new and existing encrypted data under your most recent encryption policy and keys. You can do this yourself or ask Salesforce for help.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage key material:

- [Manage Encryption Keys](#)

[Destroy Key Material](#)

Only destroy Shield Platform Encryption tenant secrets and key material in extreme cases where access to related data is no longer needed. Your key material is unique to your org and to the specific data to which it applies. Once you destroy key material, related data is not accessible unless you import previously exported key material.

[Require Multi-Factor Authentication for Key Management](#)

Multi-factor authentication (MFA) is a powerful tool for securing access to data and resources. Salesforce requires the use of MFA for all logins to your org's user interface. In addition, you can add extra security by also requiring MFA for Shield Platform Encryption key management tasks like generating, rotating, or uploading key material and certificates.

[Bring Your Own Key \(BYOK\)](#)

When you supply your own tenant secret, you get the benefits built-in to Salesforce Shield Platform Encryption, plus the extra assurance that comes from exclusively managing your tenant secret.

[Cache-Only Key Service](#)

Shield Platform Encryption's Cache-Only Key Service addresses a unique need for non-persisted key material. You can store your key material outside of Salesforce and have the Cache-Only Key Service fetch your key on demand from a key service that you control. Your key service transmits your key over a secure channel that you configure, and the Cache-Only Key Service uses your key for immediate encrypt and decrypt operations. Salesforce doesn't retain or persist your cache-only keys in any system of record or backups. You can revoke key material at any time.

SEE ALSO:

[Strengthen Your Data's Security with Shield Platform Encryption](#)

Work with Key Material

Shield Platform Encryption lets you generate a unique tenant secret for your org, or generate a tenant secret or key material using your own external resources. In either case, you manage your own key material: You can rotate it, archive it, and designate other users to share responsibility for it.

When you generate or upload new key material, any new data is encrypted using this key. This is now your active key. However, existing sensitive data remains encrypted using previous keys, which are now archived. In this situation, we strongly recommend re-encrypting this data with your active key. You can synchronize your data with the active key material on the Encryption Statistics and Data Sync.



Note: This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

SEE ALSO:

[Permission Sets](#)

[Profiles](#)

[API Guide: TenantSecret](#)

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage key material:

- [Manage Encryption Keys](#)

Rotate Your Encryption Tenant Secrets

You control the lifecycle of your data encryption keys by controlling the lifecycle of your tenant secrets. Salesforce recommends that you regularly generate or upload new Shield Platform Encryption key material. When you rotate a tenant secret, you replace it with either a Salesforce-generated tenant secret or customer-supplied key material.

Important: Where possible, we changed noninclusive terms to align with our company value of Equality. We maintained certain terms to avoid any effect on customer implementations.

To decide how often to rotate your tenant secrets, consult your security policies. How frequently you can rotate key material depends on the tenant secret type and environment. You can rotate tenant secrets one time per interval.

Table 7: Tenant Secret Rotation Intervals

Tenant Secret Type	Production Environments	Sandbox Environments
Fields and Files (Probabilistic)	24 hours	4 hours
Fields (Deterministic)	7 days	4 hours
Analytics	24 hours	4 hours
Search Index	7 days	7 days
Event Bus	7 days	7 days

The key derivation function uses a master secret, which is rotated with each major Salesforce release.

Master secret rotation doesn't impact your encryption keys or your encrypted data until you rotate your tenant secret.

1. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Key Management**.
2. In the Key Management Table, select a key type.
3. Check the status of the data type's tenant secrets. Existing tenant secrets are listed as active, archived, or destroyed.

Active

Can be used to encrypt and decrypt new and existing data.

Archived

Can't encrypt new data. Can be used to decrypt data previously encrypted with this key when it was active.

Destroyed

Can't encrypt or decrypt data. Data encrypted with this key when it was active can no longer be decrypted. Files and attachments encrypted with this key can no longer be downloaded.

4. Click **Generate Tenant Secret** or **Bring Your Own Key**. If uploading a customer-supplied tenant secret, upload your encrypted tenant secret and tenant secret hash.

Note: You can have up to 50 active and archived tenant secrets of each type. For example, you can have one active and 49 archived Fields and Files (Probabilistic) tenant secrets, and the same number of Analytics tenant secrets. This limit includes Salesforce-generated and customer-supplied key material.

If you run into this limit, destroy an existing key before reactivating, rearchiving, or creating a callout to another one. Before destroying a key, synchronize the data it encrypts with an active key.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:

- Manage Encryption Keys

- If you want to re-encrypt field values with your active key material, synchronize new and existing encrypted data under your most recent and keys. You can sync data from the Encryption Statistics and Data Sync page in Setup.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

SEE ALSO:

[API Guide: TenantSecret](#)

[Synchronize Your Data Encryption with the Background Encryption Service](#)

Back Up Your Tenant Secrets

Your Shield Platform Encryption tenant secret is unique to your org and to the specific data to which it applies. Salesforce recommends that you export your tenant secret to ensure continued access to the related data.

- From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Key Management**.
- In the table that lists your keys, find the tenant secret you want to back up. Click **Export**.
- Confirm your choice in the warning box, then save your exported file.

The file name is `tenant-secret-org-<organization ID>-ver-<tenant secret version number>.txt`. For example, `tenant-secret-org-00DD00000007eTR-ver-1.txt`.

- Note the specific version you're exporting, and give the exported file a meaningful name. Store the file in a safe location so you can import it back into your org if needed.

 **Note:** Your exported tenant secret is itself encrypted.

Remember that exported key material is a copy of the key material in your org. To import an exported tenant secret, first destroy the original in your org. See [Destroy a Tenant Secret](#) on page 973.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

SEE ALSO:

[API Guide: TenantSecret](#)

Get Statistics About Your Encryption Coverage

The Encryption Statistics page provides an overview of all data encrypted with Shield Platform Encryption. This information helps you to stay on top of your key rotation and management tasks. You can also use encryption statistics to identify which objects and fields you may want to update after you rotate your key material.

Available as an add-on subscription in: **Enterprise, Performance, and Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

EDITIONS

Available as an add-on subscription in: **Enterprise, Performance, and Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:

- Manage Encryption Keys

Gather Encryption Statistics

The Encryption Statistics and Data Sync page shows you how much of your data is encrypted by Shield Platform Encryption, and how much of that data is encrypted by active key material. Use this information to inform your key rotation actions and timelines. You can also use the Encryption Statistics page to collect information about the fields and objects you want to synchronize with the background encryption service.

Interpret and Use Encryption Statistics

The Encryption Statistics page offers a snapshot of your encrypted data. You can use the information to help make informed decisions about managing your encrypted data.

Gather Encryption Statistics

The Encryption Statistics and Data Sync page shows you how much of your data is encrypted by Shield Platform Encryption, and how much of that data is encrypted by active key material. Use this information to inform your key rotation actions and timelines. You can also use the Encryption Statistics page to collect information about the fields and objects you want to synchronize with the background encryption service.

1. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Encryption Statistics**.
2. Select an object type or custom object from the left pane. If you see a "--" in the Data Encrypted or Uses Active Key columns, you haven't gathered statistics for that object yet.

Object	Data Encrypted	Uses Active Key	Sync Needed
Account	50%	50%	Yes
Case	100%	100%	No
Contact	93%	93%	Yes
Lead	25%	25%	Yes
Opportunity	--	--	Yes
Attachment	--	--	Yes

3. Click **Gather Statistics**.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view Platform Encryption Setup pages:

- View Setup and Configuration

And

Customize Application

The gathering process time varies depending on how much data you have in your object. You're notified by email when the gathering process is finished. When your statistics are gathered, the page shows updated information about data for each object. If encryption for field history and feed tracking is turned on, you also see stats about encrypted field history and feed tracking changes.

 **Note:**

- You can gather statistics once every 24 hours, either by clicking **Gather Statistics** or running the self-service background encryption service.
- Feed Item doesn't display statistics because it's derived from Feed Post. Gathering statistics for Feed Post is sufficient to confirm the encryption status of both Feed Post and Feed Item.

SEE ALSO:

[Sync Data with Self-Service Background Encryption](#)

Interpret and Use Encryption Statistics

The Encryption Statistics page offers a snapshot of your encrypted data. You can use the information to help make informed decisions about managing your encrypted data.

Available as an add-on subscription in: **Enterprise, Performance, and Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

The page offers two views of your encrypted data: a summary view and a detail view.

Encryption Summary View

The Encryption Summary View lists all your objects that contain encrypted data, and statistics about the encrypted data in those objects.

Object	Data Encrypted	Uses Active Key	Sync Needed
Account	50%	50%	Yes
Case	100%	100%	No
Contact	93%	93%	Yes
Lead	25%	25%	Yes
Opportunity	--	--	Yes
Attachment	--	--	Yes

- Object**—Lists your standard and custom objects. Data about standard objects are aggregated for all standard objects of a given type. Data about custom objects are listed for each custom object.
- Data Encrypted**—The total percentage of data in an object that's encrypted. In the example above, 50% of all data in Account objects are encrypted.
- Uses Active Key**—The percentage of your encrypted data in that object or object type that is encrypted with your active key material.
- Sync Needed**—Recommends whether to synchronize your data with the background encryption service. This column displays Yes when you've added or disabled encryption on fields, changed a field's encryption scheme, or rotated key material.

When the numbers in both Data Encrypted and Uses Active Key columns are the same, and Sync Needed column reads No, all your encrypted data is synchronized. In the example above, the Case object is synchronized.

Sometimes the Sync Needed column reads Yes for an object when the Encrypted Data and Uses Active Key columns read have the same values. This combination of values happens when encryption policy settings or keys have changed since the last time you gathered statistics or synchronized your data. This combination also happens when statistics have been gathered for newly encrypted data, but the object has never been synchronized. In the example above, the Account, Contact, Lead, and Opportunity objects meet one or more of these conditions.

A double dash (--) means that statistics haven't been gathered for that object or object type yet. In the example, statistics haven't been gathered for the Opportunity and Attachment objects.

Encryption Detail View

The Encryption Detail View shows statistics about the field and historical data stored in each object category. If encryption for field history and feed tracking is turned on, you can also view stats about encrypted field history and feed tracking changes.

Fields

The Fields tab displays data about field data in each object.

- Field—All encryptable standard and custom fields in the object that contain data.



Note: Not all field data is stored in the same field that displays data in the UI. For example, some Person Account field data is stored in the corresponding Contact fields. If you have Person Accounts enabled but don't see encrypted fields under the Account detail view, gather statistics for the Contact object and check there.

Similarly, Chatter data is stored in the Feed Attachment, Feed Comment, Feed Poll Choice, Feed Post, and Feed Revision objects. The Encryption Statistics page lists these objects and all fields that hold encrypted Chatter data in the database. Some fields listed on the Encryption Statistics page aren't visible in the UI by the same name, but they store all encrypted data that's visible in the UI. See [Which Standard Fields Can I Encrypt?](#) in Salesforce Help for a list of the encrypted Chatter fields.

- API Name—The API name for fields that contain data.
- Encrypted Records—The number of encrypted values stored in a field type across all objects of given type. For example, you select the Account object and see "9" in the Encrypted Records column next to Account Name. That means there are nine encrypted records across all Account Name fields.
- Unencrypted Records—The number of plaintext values stored in a field type.
- Mixed Tenant Secret Status—Indicates whether a mixture of active and archived tenant secrets apply to encrypted data in a field type.
- Mixed Schemes—Indicates whether a mixture of deterministic and probabilistic encryption schemes apply to encrypted data in a field type.



Note: The following applies to both encrypted and unencrypted records:

- The records count for a field doesn't include NULL or BLANK values. A field with NULL or BLANK values can show a different (smaller) records count than the actual number of records.
- The records count for compound fields such as Contact.Name or Contact.Address can show a different (larger) records count than the actual number of records. The count includes the two or more fields that are counted for every record.

History

The History tab shows data about field history and feed tracking changes.

- Field—All encryptable standard and custom fields in the object that contain data.
- API Name—The API name for fields that contain data.

- Encrypted Field History—The number of encrypted field history values for a field type across all objects of a given type. For example, you select the Account object and see “2” in the Encrypted Field History column for Account Name, which means that Account Name has two encrypted field history values.
- Unencrypted Field History—The number of plaintext field history values stored for a field.
- Encrypted Feed Tracking—The number of encrypted feed tracking values stored for a field.
- Unencrypted Feed Tracking—The number of plaintext feed tracking values stored for a field.

Usage Best Practices

Use these statistics to make informed decisions about your key management tasks.

- Update encryption policies—The encryption statistics detail view shows you which fields in an object contain encrypted data. Use this information to periodically evaluate whether your encryption policies match your organization’s encryption strategy.
- Rotate keys—You might want to encrypt all your data with your active key material. Review the encryption summary pane on the left side of the page. If the Uses Active Key value is lower than the Data Encrypted value, some of your data uses archived key material. To synchronize your data, click the **Sync** button or contact Salesforce Customer Support.
- Synchronize data—Key rotation is an important part of any encryption strategy. When you rotate your key material, apply the active key material to existing data. To synchronize your data with your active key, click the **Sync** button.

If self-service background encryption is unavailable, review the Uses Active Key and Mixed Tenant Secret Status columns to identify any fields that include data encrypted with an archived key. Make a note of these objects and fields, then contact Salesforce Customer Support to request the background encryption service. Salesforce Customer Support can focus just on those objects and fields you want to synchronize, keeping the background encryption process as short as possible.

SEE ALSO:

[Synchronize Your Data Encryption with the Background Encryption Service](#)

Synchronize Your Data Encryption with the Background Encryption Service

Periodically, you change your encryption policy. Or you rotate your keys. To get the most protection out of your encryption strategy with Shield Platform Encryption, synchronize new and existing encrypted data under your most recent encryption policy and keys. You can do this yourself or ask Salesforce for help.

When a change occurs, you have options for keeping your encryption policy up to date. You can synchronize most standard and custom field data yourself from the Encryption Statistics and Data Sync page in Setup. For all other data, Salesforce is here to help ensure data alignment with your latest encryption policy and tenant secret.

When We Do and Don't Automatically Encrypt Your Data

- When you turn on encryption for specific fields or other data, newly created and edited data are automatically encrypted with the most recent key.
- Data that's already in your org doesn't automatically get encrypted. Our background encryption service takes care of that on request.
- When you change your tenant secret as part of your key rotation strategy, data that's already encrypted remains encrypted with the old tenant secret. Our background encryption service can update it on request. And don't worry, you always have access to your data as long as you don't destroy the old, archived keys.
- If you turn off encryption, data that's already there is automatically decrypted based on the relevant key. Any functionality impacted by having encrypted data is restored.
- If Salesforce support re-encrypts your data with a new key, any data that was encrypted with the destroyed key is skipped. To access data encrypted with a destroyed key, import a backup of the destroyed key.

 **Note:** Note: Synchronizing your data encryption doesn't modify the record LastModifiedDate or LastModifiedById timestamps. It doesn't execute triggers, validation rules, workflow rules, or any other automated service. However, it does modify the SystemModStamp.

What You Can Synchronize Yourself

You can synchronize most encrypted data yourself from the Encryption Statistics page in Setup. Self-service background encryption synchronizes:

- Standard and custom fields
- The Attachment—Content Body field
- Field history and feed tracking changes when the **Encrypt Field History and Feed Tracking Values** setting is turned on

Read more about [self-service background encryption](#) on page 972, and its [considerations](#) on page 1003, in Salesforce Help.

How to Request Background Encryption Service from Salesforce Customer Support

If you can't sync data yourself, contact Salesforce Customer Support for help. Keep these tips in mind when asking for help with syncing your data.

Allow lead time

Contact Salesforce support 2–3 business days before you need the background encryption completed. The time to complete the process varies based on the volume of data. It could take several days.

Specify the data

Provide the list of objects, field names, and data elements you want encrypted or re-encrypted.

Verify the list

Verify that this list matches what's encrypted in Setup:

- Data elements selected on the Encryption Policy page
- Standard fields selected on the Encrypt Standard Fields page
- Custom fields you selected for encryption on the Field Definition page

 **Tip:** Also check that your field values aren't too long for encryption.

Include files and attachments?

Encryption for files and attachments is all or nothing. You don't have to specify which ones.

Include history and feed data?

Specify whether you want the corresponding field history and feed data encrypted.

Choose a time

Salesforce Customer Support can run the background encryption service Monday through Friday between 6 AM and 5 PM in your time zone.

 **Tip:** If you're not sure which data is already encrypted, visit the Encryption Statistics page, which keeps a record of all fields that you have encrypted.

What If You Destroyed Your Key?

If your encryption key has been destroyed, your data can't be automatically decrypted. You have some options for handling this data.

- Reimport the destroyed key from a backup, then ask Salesforce Customer Support to synchronize your data with your encryption policy.

- Delete all the data that was encrypted with the destroyed key, then ask Salesforce Customer Support to synchronize your data.
 - Ask Salesforce Customer Support to mass overwrite the data that was encrypted with the destroyed key with "?????".
-  **Note:** Keep these points in mind when disabling encryption on data encrypted with destroyed material.
- When you disable encryption for files that were encrypted with a key that's been destroyed, the files don't automatically go away. You can ask Salesforce support to delete the files.
 - The automatic decryption process takes longer when you disable encryption on fields encrypted with a key that's been destroyed. Salesforce notifies you by email when the process finishes.

Sync Data with Self-Service Background Encryption

Synchronizing your data with your active key material keeps your encryption policy up to date. You can sync data in standard and custom fields, the Attachment—Content Body field, and for field history and feed tracking changes from the Encryption Statistics and Data Sync page in Setup. To synchronize all other encrypted data, contact Salesforce Customer Support.

SEE ALSO:

- [General Shield Platform Encryption Considerations](#)
- [Field Limits with Shield Platform Encryption](#)
- [Disable Encryption on Fields](#)

Sync Data with Self-Service Background Encryption

Synchronizing your data with your active key material keeps your encryption policy up to date. You can sync data in standard and custom fields, the Attachment—Content Body field, and for field history and feed tracking changes from the Encryption Statistics and Data Sync page in Setup. To synchronize all other encrypted data, contact Salesforce Customer Support.

Self-service background encryption supports all standard and custom fields, the Attachment—Content Body field, and field history and feed tracking changes. For help synchronizing other encrypted data, contact Salesforce Customer Support.

To include field history and feed tracking values in self-service background encryption processes, first turn on **Encrypt Field History and Feed Tracking Values** on the Encryption Settings page. You can also enable field history and feed tracking encryption programmatically with the [PlatformEncryptionSettings](#) metadata type. When this setting is turned on, the self-service background encryption process applies your active key material to your field history and feed tracking values.

1. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Encryption Statistics**.
2. Select an object type or custom object from the left pane.

 **Note:** The Sync Needed column indicates when to synchronize your data. This column displays Yes when you add or remove encryption on fields, rotate keys, or change a field's encryption scheme.

3. Click **Sync**.
Supported standard and custom fields are encrypted with your active key material and encryption policy in the background. After the service syncs your data, it gathers statistics for the object. To view your gathered statistics, wait for your verification email and then refresh the Encryption Statistics and Data Sync page.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

View Platform Encryption Setup pages:

- [View Setup and Configuration](#)

 **Note:** The sync process time varies depending on how much data you have in your object. You get an email notification when the sync process finishes. You can sync your data from the Encryption Statistics and Data Sync page once every 7 days.

If you have lots of data in Attachment—Content Body fields, the sync process breaks your request into batches and syncs them in sequence. However, sometimes we can't encrypt all these batches at once. This service protection helps Salesforce maintain functional network loads. If the sync process finishes but the encryption statistics status is less than 100% complete, click **Sync** again. The background encryption service picks up where it left off.

Destroy Key Material

Only destroy Shield Platform Encryption tenant secrets and key material in extreme cases where access to related data is no longer needed. Your key material is unique to your org and to the specific data to which it applies. Once you destroy key material, related data is not accessible unless you import previously exported key material.

You are solely responsible for making sure that your data and key material are backed up and stored in a safe place. Salesforce can't help you with deleted, destroyed, or misplaced tenant secrets and keys.

1. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Key Management**.
2. In the table that lists your tenant secrets, find the row that contains the one you want to destroy. Click **Destroy**.
3. A warning box appears. Type in the text as shown and select the checkbox acknowledging that you're destroying a tenant secret, then click **Destroy**.
After you destroy the key that encrypted the content, file previews and content that was already cached in the user's browser may still be visible in cleartext. When the user logs in again, the cached content is removed.

If you create a sandbox org from your production org and then destroy the tenant secret in your sandbox org, the tenant secret still exists in the production org.
4. To import your tenant secret, click **Import > Choose File** and select your file. Make sure you're importing the correct version of the tenant secret.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

Require Multi-Factor Authentication for Key Management

Multi-factor authentication (MFA) is a powerful tool for securing access to data and resources. Salesforce requires the use of MFA for all logins to your org's user interface. In addition, you can add extra security by also requiring MFA for Shield Platform Encryption key management tasks like generating, rotating, or uploading key material and certificates.

 **Important:** Make sure that you provide security administrators a way to get a time-based, one-time password. This password is their second authentication factor (in addition to their Salesforce username and password). Otherwise, they can't complete encryption key-related tasks.

1. From Setup, in the Quick Find box, enter *Identity Verification*, and then select **Identity Verification**.

EDITIONS

Available as an add-on subscription in: **Enterprise, Performance, and Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:

- Manage Encryption Keys

EDITIONS

Available in: **Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To assign identity verification for key management tasks:

- Manage Encryption Keys

2. Select **Raise session to high-assurance** from the Manage Encryption Keys dropdown. All admins with the Manage Encryption Keys permission must use an additional verification method to complete key management tasks through Setup and the API.

Bring Your Own Key (BYOK)

When you supply your own tenant secret, you get the benefits built-in to Salesforce Shield Platform Encryption, plus the extra assurance that comes from exclusively managing your tenant secret.

Controlling your own tenant secret entails contacting Salesforce Customer Support to enable Bring Your Own Keys, generating a BYOK-compatible certificate, using that certificate to encrypt and secure your self-generated tenant secret, then granting the Salesforce Shield Platform Encryption key management machinery access to your tenant secret.

1. [Bring Your Own Key Overview](#)

Yes. You can generate and store your customer-supplied key material outside of Salesforce using your own crypto libraries, enterprise key management system, or hardware security module (HSM). You then grant the Salesforce Shield Platform Encryption key management machinery access to those keys. You can choose to encrypt your keys with a public key from a self-signed or CA-signed certificate.

2. [Generate a BYOK-Compatible Certificate](#)

To encrypt data in Salesforce with Bring Your Own Key (BYOK) key material, use Salesforce to generate a 4096-bit RSA certificate. You can generate a self-signed or certificate-authority (CA) signed certificate. Each BYOK-compatible certificate's private key is encrypted with a derived, org-specific tenant secret key.

3. [Generate and Wrap BYOK Key Material](#)

Generate a random number as your BYOK tenant secret. Then calculate an SHA256 hash of the secret, and encrypt it with the public key from the BYOK-compatible certificate you generated.

4. [Sample Script for Generating a BYOK Tenant Secret](#)

We've provided a helper script that may be handy for preparing your tenant secret for upload. The script generates a random number as your tenant secret, calculates an SHA256 hash of the secret, and uses the public key from the certificate to encrypt the secret.

5. [Upload Your BYOK Tenant Secret](#)

After you have your BYOK-compatible tenant secret, upload it to Salesforce. The Shield Key Management Service (KMS) uses your tenant secret to derive your org-specific data encryption key.

6. [Opt Out of Key Derivation with BYOK](#)

If you don't want Shield Platform Encryption to derive a data encryption key for you, you can opt out of key derivation and upload your own final data encryption key. Opting out gives you even more control of the key material used to encrypt and decrypt your data.

7. [Take Good Care of Your BYOK Keys](#)

When you create and store your own key material outside of Salesforce, it's important that you safeguard that key material. Make sure that you have a trustworthy place to archive your key material; never save a tenant secret or data encryption key on a hard drive without a backup.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, and upload tenant secrets and customer-supplied key material:

- Manage Encryption Keys

To edit, upload, and download HSM-protected certificates with the Shield Platform Encryption Bring Your Own Key service:

- Manage Encryption Keys
- AND
- Manage Certificates
- AND
- Customize Application

8. [Troubleshooting Bring Your Own Key](#)

One or more of these frequently asked questions may help you troubleshoot any problems that arise with Shield Platform Encryption's Bring Your Own Key service.

SEE ALSO:

[Key Management and Rotation](#)

Bring Your Own Key Overview

Yes. You can generate and store your customer-supplied key material outside of Salesforce using your own crypto libraries, enterprise key management system, or hardware security module (HSM). You then grant the Salesforce Shield Platform Encryption key management machinery access to those keys. You can choose to encrypt your keys with a public key from a self-signed or CA-signed certificate.

To work with our key management machinery, your customer-supplied key material must meet these specifications:

- 256-bit size
- Encrypted with a public RSA key that is extracted from the downloaded BYOK certificate, then padded using OAEP padding
- After it's encrypted, it must be encoded in standard base64

To work with encryption keys, you need the Manage Encryption Keys permission. To generate BYOK-compatible certificates, you need the Customize Application permission.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Generate a BYOK-Compatible Certificate

To encrypt data in Salesforce with Bring Your Own Key (BYOK) key material, use Salesforce to generate a 4096-bit RSA certificate. You can generate a self-signed or certificate-authority (CA) signed certificate. Each BYOK-compatible certificate's private key is encrypted with a derived, org-specific tenant secret key.

To create a self-signed certificate:

1. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Key Management**.
2. Click **Bring Your Own Key**.
3. Click **Create Self-Signed Certificate**.
4. Enter a unique name for your certificate in the Label field. The Unique Name field automatically assigns a name based on what you enter in the Label field.

The Exportable Private Key (1), Key Size (2), and Use Platform Encryption (3) settings are pre-set. These settings ensure that your self-signed certificate is compatible with Salesforce Shield Platform Encryption.

5. When the Certificate and Key Detail page appears, click **Download Certificate**.

If you're not sure whether a self-signed or CA-signed certificate is right for you, consult your organization's security policy. See [Certificates and Keys](#) in Salesforce Help for more about what each option implies.

To create a CA-signed certificate, follow the instructions in the [Generate a Certificate Signed By a Certificate Authority](#) topic in Salesforce Help. Remember to manually change the **Exportable Private Key**, **Key Size**, and **Platform Encryption** settings to ensure that your certificate is BYOK-compatible.

SEE ALSO:

[Certificates and Keys](#)

[Generate a Certificate Signed by a Certificate Authority](#)

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:

- Manage Encryption Keys

Edit, upload, and download HSM-protected certificates with the Shield Platform Encryption Bring Your Own Key service

- Manage Certificates

AND

Customize Application

AND

Manage Encryption Keys

Generate and Wrap BYOK Key Material

Generate a random number as your BYOK tenant secret. Then calculate an SHA256 hash of the secret, and encrypt it with the public key from the BYOK-compatible certificate you generated.

1. Generate a 256-bit tenant secret using the method of your choice.
You can generate your tenant secret in one of 2 ways:
 - Use your own on-premises resources to generate a tenant secret programmatically, using an open-source library such as Bouncy Castle or OpenSSL.
 -  **Tip:** We've provided a script on page 977 that may be useful as a guide to the process.
 - Use a key brokering partner that can generate, secure, and share access to your tenant secret.
2. Wrap your tenant secret with the public key from the BYOK-compatible certificate you generated, using the default SHA1 padding algorithm.
Specify the OAEP padding scheme. Make sure the resulting encrypted tenant secret and hashed tenant secret files are encoded using base64.
3. Encode this encrypted tenant secret to base64.
4. Calculate an SHA-256 hash of the plaintext tenant secret.
5. Encode the SHA-256 hash of the plaintext tenant secret to base64.

Sample Script for Generating a BYOK Tenant Secret

We've provided a helper script that may be handy for preparing your tenant secret for upload. The script generates a random number as your tenant secret, calculates an SHA256 hash of the secret, and uses the public key from the certificate to encrypt the secret.

1. Download the script from the [Salesforce Knowledge Base](#). Save it in the same directory as the certificate.
2. Run the script specifying the certificate name, like this: `./secretgen.sh my_certificate.crt`
Replace this certificate name with the actual filename of the certificate you downloaded.
 -  **Tip:** If needed, use `chmod +w secretgen.sh` to make sure that you have write permission to the file and use `chmod 775` to make it executable.
3. The script generates several files. Look for the two files that end with the .b64 suffix. The files ending in .b64 are your base 64-encoded encrypted tenant secret and base 64-encoded hash of the plaintext tenant secret. You'll need both of these files for the next step.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

Edit, upload, and download HSM-protected certificates with the Shield Platform Encryption Bring Your Own Key service:

- Manage Certificates
- AND
- Customize Application
- AND
- Manage Encryption Keys

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Upload Your BYOK Tenant Secret

After you have your BYOK-compatible tenant secret, upload it to Salesforce. The Shield Key Management Service (KMS) uses your tenant secret to derive your org-specific data encryption key.

1. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Key Management**.
2. In the Key Management Table, select a key type.
3. Click **Bring Your Own Key**.
4. In the Upload Tenant Secret section, attach both the encrypted key material and the hashed plaintext key material. Click **Upload**.

This tenant secret automatically becomes the active tenant secret.

Your tenant secret is now ready to be used for key derivation. From here on, the Shield KMS uses your tenant secret to derive an org-specific data encryption key. The app server then uses this key to encrypt and decrypt your users' data.

If you don't want Salesforce to derive a data encryption key for you, you can opt out of key derivation and upload your own final data encryption key. For more information, see [Opt-Out of Key Derivation with BYOK in Salesforce Help](#).

 **Note:** You can have up to 50 active and archived tenant secrets of each type. For example, you can have one active and 49 archived Fields and Files (Probabilistic) tenant secrets, and the same number of Analytics tenant secrets. This limit includes Salesforce-generated and customer-supplied key material.

If you reach the limit, destroy an existing key before reactivating, rearchiving, or creating a callout to another one. Before destroying a key, synchronize the data that it encrypts with an active key.

5. Export your tenant secret, and back it up as prescribed in your organization's security policy.

To restore a destroyed tenant secret, reimport it. The exported tenant secret is different from the tenant secret you uploaded. It's encrypted with a different key and has additional metadata embedded in it. See [Back Up Your Tenant Secret](#) in Salesforce Help.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, and upload tenant secrets and customer-supplied key material:

- Manage Encryption Keys

Opt Out of Key Derivation with BYOK

If you don't want Shield Platform Encryption to derive a data encryption key for you, you can opt out of key derivation and upload your own final data encryption key. Opting out gives you even more control of the key material used to encrypt and decrypt your data.

Generate your customer-supplied data encryption key using a method of your choice. Then calculate an SHA256 hash of the key, and encrypt it with the public key from a BYOK-compatible certificate. See [Upload Your BYOK Tenant Secret](#) for details about how to prepare customer-supplied key material.

1. Make sure that your org has the Bring Your Own Keys feature enabled. To enable this feature, contact Salesforce Customer Support.
2. From Setup, in the Quick Find box, enter *Encryption Settings*, and then select **Encryption Settings**.
3. In the Advanced Encryption Settings section, turn on **Allow BYOK to Opt-Out of Key Derivation**.

You can also enable the Allow BYOK to Opt-Out of Key Derivation setting programmatically. For more information, see [EncryptionKeySettings](#) in the *Metadata API Developer Guide*.

You can now opt out of key derivation when you upload key material.

4. From Setup, in the Quick Find box, enter *Key Management*, and then select **Key Management**.
5. In the Key Management Table, select a key type.
6. Click **Bring Your Own Key**.
7. Deselect **Use Salesforce key derivation**.

8. In the Upload Tenant Secret section, attach both your encrypted data encryption key and your hashed plaintext data encryption key.
9. Click **Upload**.
This data encryption key automatically becomes the active key. From now on, the Shield Key Management Service (KMS) skips the derivation process and uses your data encryption key to directly encrypt and decrypt your data. You can review the derivation status of all key material on the Key Management page.
10. Export your data encryption key and back it up as prescribed in your organization's security policy.

To restore your data encryption key, reimport it. The exported data encryption key is different from the data encryption key you uploaded. It's encrypted with a different key and has additional metadata embedded in it. See [Back Up Your Tenant Secret](#) in Salesforce Help.

Note: This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, and upload tenant secrets and customer-supplied key material:

- Manage Encryption Keys

To allow BYOK to opt out of key derivation:

- Customize Application

AND

- Manage Encryption Keys

Take Good Care of Your BYOK Keys

When you create and store your own key material outside of Salesforce, it's important that you safeguard that key material. Make sure that you have a trustworthy place to archive your key material; never save a tenant secret or data encryption key on a hard drive without a backup.

Back up all imported key material after you upload them to Salesforce. This ensures that you have copies of your active key material. See [Back Up Your Tenant Secret](#) in Salesforce Help.

Review your company policy on key rotation. You can rotate and update your keys on your own schedule. See [Rotate Your Encryption Keys](#).

Important: If you accidentally destroy a tenant secret that isn't backed up, Salesforce won't be able to help you retrieve it.

Troubleshooting Bring Your Own Key

One or more of these frequently asked questions may help you troubleshoot any problems that arise with Shield Platform Encryption's Bring Your Own Key service.

I'm trying to use the script you provide, but it won't run.

Make sure that you are running the right script for your operating system. If you are working on a Windows machine, you can install a Linux emulator and use the Linux script. These issues can also prevent the script from running:

- You don't have write permission in the folder you're trying to run the script from. Try running the script from a folder that you have write permission for.
- The certificate that the script references is missing. Make sure you've properly generated the certificate.
- The certificate is missing or is not being referenced by the correct name. Make sure you've entered the correct file name for your certificate in the script.

I want to use the script you provide, but I also want to use my own random number generator.

The script we provide uses a random number generator to create a random value that is then used as your tenant secret. If you would like to use a different generator, replace `head -c 32 /dev/urandom | tr '\n' =` (or, in the Mac version, `head -c 32 /dev/urandom > $PLAINTEXT_SECRET`) with a command that generates a random number using your preferred generator.

What if I want to use my own hashing process to hash my tenant secret?

No problem. Just make sure that the result meets these requirements:

- Uses an SHA-256 algorithm.
- Results in a base64 encoded hashed tenant secret.
- Generates the hash of the random number BEFORE encrypting it.

If any of these three criteria aren't met, you can't upload your tenant secret.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

How should I encrypt my tenant secret before I upload it to Salesforce?

If you're using the script provided, the encryption process is taken care of. If you do not use the script, specify the OAEP padding scheme when you encrypt your tenant secret. Make sure the resulting encrypted tenant secret and hashed tenant secret files are encoded using base64. If either of these criteria are not met, you can't upload your tenant secret.

If you choose to not use the script provided, follow the instructions in the [Generate And Wrap Your Tenant Secret Help](#) topic.

I can't upload my Encrypted tenant secret and Hashed tenant secret.

A handful of errors can prevent your files from uploading. Use the chart to make that sure your tenant secrets and certificates are in order.

Possible cause	Solution
Your files were generated with an expired certificate.	Check the date on your certificate. If it has expired, you can renew your certificate or use another one.
Your certificate is not active, or is not a valid Bring Your Own Key certificate.	Ensure that your certificate settings are compatible with the Bring Your Own Key feature. Under the Certificate and Key Edit section of the Certificates page, select a 4096-bit certificate size, disable Exportable Private Key, and enable Platform Encryption.
You haven't attached both the encrypted tenant secret and the hashed tenant secret.	Make sure that you attach both the encrypted tenant secret and hashed tenant secret. Both of these files should have a .b64 suffix.
Your tenant secret or hashed tenant secret wasn't generated properly.	Several problems can cause this error. Usually, the tenant secret or hashed tenant secret wasn't generated using the correct SSL parameters. If you are using OpenSSL, you can refer to the script for an example of the correct parameters you should use to generate and hash your tenant secret. If you are using a library other than OpenSSL, check that library's support page for help with finding the correct parameters to both generate and hash your tenant secret. Still stuck? Contact your Salesforce account executive. They'll put you in touch with someone at Salesforce who can help.

I'm still having problems with my key. Who should I talk to?

If you still have questions, contact your account executive. They'll put you in touch with a support team specific to this feature.

SEE ALSO:

[Key Management and Rotation](#)

Cache-Only Key Service

Shield Platform Encryption's Cache-Only Key Service addresses a unique need for non-persisted key material. You can store your key material outside of Salesforce and have the Cache-Only Key Service fetch your key on demand from a key service that you control. Your key service transmits your key over a secure channel that you configure, and the Cache-Only Key Service uses your key for immediate encrypt and decrypt operations. Salesforce doesn't retain or persist your cache-only keys in any system of record or backups. You can revoke key material at any time.

1. [How Cache-Only Keys Works](#)

The Shield Platform Encryption Cache-Only Key Service lets you use a variety of key services to generate, secure, and store your key material. You can use an on-premises key service, host your own cloud-based key service, or use a cloud-based key brokering vendor.

2. [Prerequisites and Terminology for Cache-Only Keys](#)

Shield Platform Encryption's Cache-Only Key Service offers you more control over your key material. When you use cache-only keys, you control more of the key management tasks. Before you start using the service, understand how to create and host your key material in a way that's compatible with Salesforce's BYOK service.

3. [Create and Assemble Your Key Material](#)

The Shield Platform Encryption Cache-Only Key Service is compatible with 256-bit AES keys returned in a JSON response, and then wrapped using JSON Web Encryption (JWE).

4. [Configure Your Cache-Only Key Callout Connection](#)

Use a named credential to specify the endpoint for your callout, and identify the key that you want to fetch from your endpoint.

5. [Add Replay Detection for Cache-Only Keys](#)

Replay detection protects your cache-only keys if a callout is fraudulently intercepted. When enabled, replay detection inserts an autogenerated, unique marker called a RequestIdentifier into every callout. The RequestIdentifier includes the key identifier, a nonce generated for that callout instance, and the nonce required from the endpoint. The RequestIdentifier serves as a random, one-time identifier for each valid callout request. After you set up your key service to accept and return the RequestIdentifier, any callout with missing or mismatched RequestIdentifiers is aborted.

6. [Check Your Cache-Only Key Connection](#)

Because your cache-only key material is stored outside of Salesforce, it's important to maintain a functional callout connection. Use the Callout Check page to monitor your connection and quickly respond to key service interruptions that could prevent the service from fetching your keys.

7. [Destroy a Cache-Only Key](#)

When you destroy a cache-only key, you're destroying two things: the key in the cache and the callout connection to the key service.

8. [Reactivate a Cache-Only Key](#)

If you still have your named credential associated with a key that was destroyed in Salesforce, you can reactivate a destroyed cache-only key from Setup or programmatically through the API. Reactivating a destroyed key makes it the active key. Before you reactivate a destroyed key, make sure that the corresponding key service connection is recovered.

9. [Considerations for Cache-Only Keys](#)

These considerations apply to all data that you encrypt using the Shield Platform Encryption Cache-Only Key Service.

EDITIONS

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions. Requires purchasing Salesforce Shield or Shield Platform Encryption, and the Cache-Only Key Service.

Available in both Salesforce Classic and Lightning Experience.

10. [Troubleshoot Cache-Only Keys](#)

One or more of these frequently asked questions may help you troubleshoot any problems that arise with Shield Platform Encryption's Cache-Only Key Service.

SEE ALSO:

[Key Management and Rotation](#)

How Cache-Only Keys Works

The Shield Platform Encryption Cache-Only Key Service lets you use a variety of key services to generate, secure, and store your key material. You can use an on-premises key service, host your own cloud-based key service, or use a cloud-based key brokering vendor.

Figures 1 and 2 show how Salesforce fetches keys on-demand from your specified key service. Whether you store your keys with an on-premises key service or a cloud-based key service, the flow is the same. When users access encrypted data, or add sensitive data to encrypted data elements, the Cache-Only Key Service makes a callout to your key service. Your key service passes key material, wrapped securely in JSON Web Encryption format, through a secure, authenticated channel that you set up.

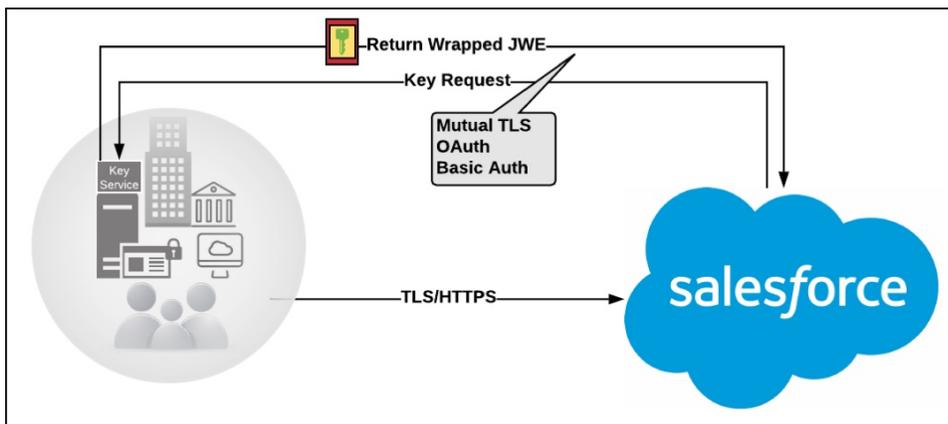


Figure 1: On-premises Key Service

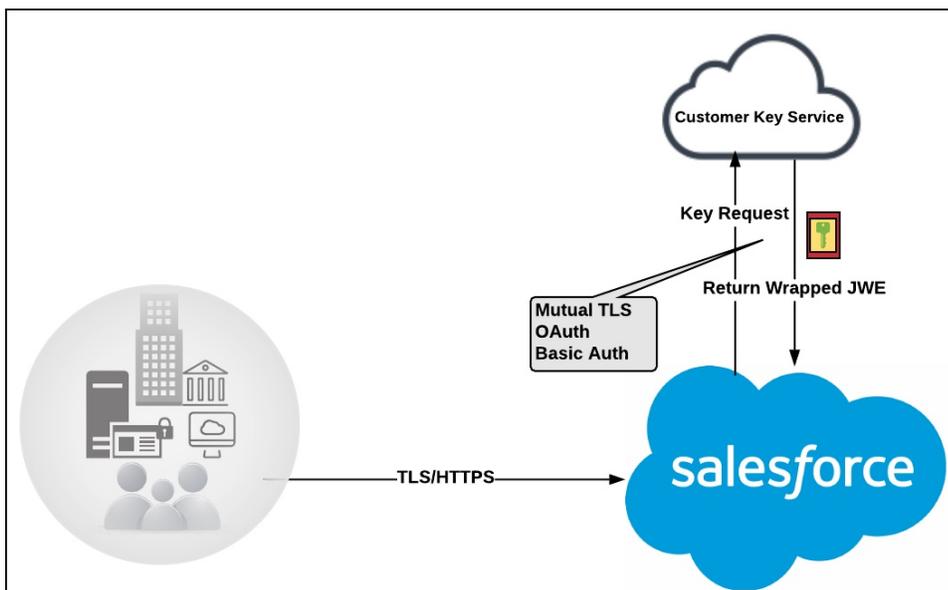


Figure 2: Cloud-Based Key Service

As a core offering of the Shield KMS, enhanced cache controls ensure that key material is stored securely while in the cache. The Shield KMS encrypts the fetched key material with an org-specific AES 256-bit cache encryption key and stores the encrypted key material in the cache for encrypt and decrypt operations. HSM-protected keys secure the cache encryption key in the cache, and the cache encryption key is rotated along with key lifecycle events such as key destruction and rotation.

The enhanced cache controls provide a single source of truth for key material used to encrypt and decrypt your data. Subsequent encryption and decryption requests go through the encrypted key cache until the cache-only key is revoked or rotated, or the cache is flushed. Once the cache is flushed, the Cache-Only Key Service fetches key material from your specified key service. The cache is regularly flushed every 72 hours, and certain Salesforce operations flush the cache on average every 24 hours. Destroying a data encryption key invalidates the corresponding data encryption key that's stored in the cache.

Because cache-only keys bypass the key derivation process, they're used to directly encrypt and decrypt your data.

Prerequisites and Terminology for Cache-Only Keys

Shield Platform Encryption's Cache-Only Key Service offers you more control over your key material. When you use cache-only keys, you control more of the key management tasks. Before you start using the service, understand how to create and host your key material in a way that's compatible with Salesforce's BYOK service.

Prerequisites

- Prepare your Salesforce org. Make sure that your org has at least one active Data in Salesforce key, either Salesforce-generated or customer-supplied. You can create a tenant secret by clicking **Generate Tenant Secret** on the Key Management page in Setup.
- Generate and Host Key Material. The cache-only key exchange protocol and format requires that keys are wrapped in an opinionated JSON Web Encryption (JWE). This format uses RSAES-OAEP for key encryption and AES GCM for content encryption.

Use a secure, trusted service to generate, store, and back up your key material.

- Use and maintain a reliable high-availability key service. Choose a high-availability key service with an acceptable service level agreement (SLA), predefined maintenance procedures, and processes to mitigate any potential impact to business continuity.

When the connection between Salesforce and your key service is broken, the Cache-Only Key Service can encrypt and decrypt data as long as your key material is in the cache. However, keys don't stay in the cache for long. The cache is regularly flushed every 72 hours, but some Salesforce operations flush the cache about every 24 hours.

If your key material isn't in the cache, and the connection to your key service is broken, users can't encrypt or decrypt records. Make sure that you use a key service that Salesforce can connect to at any time. This is especially important during busy times like the end of year or end of quarter.

- Maintain a secure callout endpoint. The cache-only key exchange protocol requires that keys are wrapped in an opinionated JSON format. Host your wrapped key inside the key response at a location Salesforce can request.

The Cache-Only Key Service uses named credentials to establish a secure, authenticated connection to [allowed IP addresses and domains](#). You can configure your named credentials to use popular authentication formats, such as Mutual TLS and OAuth. You can change these authentication protocols at any time.

- Actively monitor your key service logs for errors. While Salesforce is here to help you with the Shield Platform Encryption service, you are responsible for maintaining the high-availability key service that you use to host your key material. You can use the [RemoteKeyCalloutEvent](#) object to review or track cache-only key events.



Warning: Because you're in control of your keys, you're responsible for securing and backing up your key material. Salesforce can't retrieve lost key material stored outside of our encrypted key cache.

- Know how to format and assemble your key material. Format key material hosted outside of Salesforce in a way that's compatible with the Cache-Only Key Service. Make sure that you can generate the following components in the required formats.

Table 8: Cache-Only Key Components

Component	Format
Data encryption key (DEK)	AES 256-bit
Content encryption key (CEK)	AES 256-bit
BYOK-compatible certificate	A 4096-bit RSA certificate whose private key is encrypted with a derived, org-specific tenant secret key
JSON Web Encryption content and header	See a sample in Github
Algorithm for encrypting the CEK	RSA-OAEP
Algorithm for encrypting the DEK	A256GCM
Unique key identifier	Allows numbers, uppercase and lowercase letters, periods, hyphens, and underscores
Initialization vector	Encoded in base64url
JSON web token ID (JTI)	A 128-bit hex encoded, randomly generated identifier

Read more about assembling your key material in the Generate and Assemble Cache-Compatible Keys section. You can also look at our [Cache-Only Key Wrapper](#) in Github for examples and sample utility.

Terminology

Here are some terms that are specific to the Cache-Only Key Service.

Content Encryption Key

For each key request, your key service endpoint generates a unique content encryption key. The content encryption key wraps the data encryption key, which is in turn encrypted by the key encrypting key and placed in the JWE header of the key response.

JSON Web Encryption

The JSON-based structure that the Shield Platform Encryption service uses to encrypted content. JSON Web Encryption, or JWE, uses RSAES-OAEP for key encryption and AES GCM for content encryption.

JSON Web Token ID

A unique identifier for the JSON web token, which enables identity and security information to be shared across security domains.

Key Identifier

The Key ID, or KID, is the unique identifier for your key. The KID is used as the suffix in the named credential and for validation of the KID in the response. In Setup, enter this identifier in the Unique Key Identifier field.

Create and Assemble Your Key Material

The Shield Platform Encryption Cache-Only Key Service is compatible with 256-bit AES keys returned in a JSON response, and then wrapped using JSON Web Encryption (JWE).

Cache-only key material is wrapped in a JSON format. An example cache-only key is used throughout this article to illustrate how key material changes as you assemble it.

1. Generate a 256-bit AES data encryption key. You can use the cryptographically secure method of your choice.
2. Generate a 256-bit AES content encryption key using a cryptographically secure method.
3. Generate and download your BYOK-compatible certificate.
4. Create the JWE protected header. The JWE protected header is a JSON object with 3 claims: the algorithm used to encrypt the content encryption key, the algorithm used to encrypt the data encryption key, and the unique ID of the cache-only key. Here's an example header to get us started.

```
{"alg": "RSA-OAEP", "enc": "A256GCM", "kid": "982c375b-f46b-4423-8c2d-4d1a69152a0b" }
```

5. Encode the JWE protected header as BASE64URL(UTF8(JWE Protected Header)).

```
eyJhbGciOiJSU0EtT0FFUCIsImVuYyI6IkJEYNTZHQ00iLCJraWQiOiI5ODJjMzc1Yi1mNDZiLTQ0MjMtOGMyZC00ZDFhNjknNTJhMGIifQ
```

6. Encrypt the content encryption key with the public key from the BYOK certificate using the RSAES-OAEP algorithm. Then encode this encrypted content encryption key as BASE64URL(Encrypted CEK).

```
192QA-R7b6Gtjo0tG4GlylJti1-Pf-519YpStYOp28YToMxgUxPmx4NR_myvfT24oBCwkh6hy_dqAL7JlVO449EgLAB_i9GRdyVbTKnJQ1OivKwWUQaZ9jVNxFFUYTWwZ-sVK4pUw0B3lHwWBfpMs14jf0exp5-5amiTZ5oP0rkW99ugLWJ_7XlyTuMIA6VTLSpL0YqChH1wQjo12TQaWG_tiTwl1SgRd3YohuMv1mCdEmR2TfwTvrYLpX4KbFK3Pv5ZSpSIyreFTh12DPpmhLEAVhCBZxR4-HMnZySSs4QorWagOaT8XPjPv46m8mUATZSD4hab8v3Mq4H33CmwngZCJXX-sDHuax2JUejxNC8HT5p6sa_I2gQFM1BC2Sd4yBKyj1DQKcSs1CVav4buG8hkOJXY69iW_zhztV3DoJJ901-EvkMoHpw111U91FhJMUQRv vocfghs2kzy5QC8QQt4t4Wu3p7IvzeneL5I81QjQ1DJmZhbLLorFHgcAs9_FMwnFYFrgsHP1_v3Iqy7zJjc60fCfDaxAF8Txj_L0eOMkCF1-9PwrULWyRTLMI7CdZIm7jb8v9ALxcmDgqU11yvEeBJhgMLezAWtxvGGkejc0BdsbWapFX1I3Uj7C-Mw8LcmpSLKZyEnhj2x-3Vfv5hIVauC6ja1B6Z_UcqXK0c
```

7. Generate an initialization vector for use as input to the data encryption key's AES wrapping. Then encode it in base64url.

```
N2WVMbpAxipAtG90
```

8. Wrap your data encryption key with your content encryption key.

- a. Encode the JWE header as ASCII(BASE64URL(UTF8(JWE Protected Header))).
- b. Reform authenticated encryption on the data encryption key with the AES GCM algorithm. Use the content encryption key as the encryption key, the initialization vector (the bytes, not the base64URL encoded version), and the Additional Authenticated Data value, requesting a 128-bit Authentication Tag output.
- c. Encode the resulting ciphertext as BASE64URL(Ciphertext).
- d. Encode the Authentication Tag as BASE64URL(Authentication Tag).

```
63wRVVKX0ZOxu8cKqN1kqN-7EDa_mnmk32DinS_zFo4
```

EDITIONS

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions. Requires purchasing Salesforce Shield or Shield Platform Encryption, and the Cache-Only Key Service.

Available in both Salesforce Classic and Lightning Experience.

and

```
HC7Ev5lmsbTgwyGpeGH5Rw
```

- Assemble your JWE as a compact serialization of all the preceding values. Concatenate values separated by a period.

```
eyJhbGciOiJSU0EtT0FFUCIsImVuYyI6IkeYNTZHQ00iLCJraWQiOiI5ODJjMzc1Yi1mNDZiLTQ0MjMtOGMyZC00ZDFhNjknNTJhMGIifQ.192QA-R7b6Gtjo0tG4GlylJt1l-Pf-519YpStYOp28YToMxgUxPmx4NR_myvfT24oBCWkh6hy_dqAL7JlVO449EglAB_i9GRdyVbTKnJQ10iVKwWUQaz9jVNxFFUYTWWZ-sVK4pUw0B3lHwWBfpMsl4jF0exP5-5amiTZ5oP0rkW99ugLWJ_7XlyTuMIA6VTLSpL0YqChHlwQjo12TQaWG_tiTwl1SgRd3YohuMv1mCdEmR2TfwTvryLPx4KbFK3Pv5ZSpSIyreFTh12DPpmhLEAVhCBZxR4-HMnZySSs4QorWagOaT8XPjPv46m8mUATZSD4hab8v3Mq4H33CmwngZCJXX-sDHuax2JUejxNC8HT5p6sa_I2gQFM1BC2Sd4yBKyj1DQKcSslCVav4buG8hkOJXY69iW_zhztV3DoJJ901-EvkMoHpw111U91FhJMUQRvvocfghs2kzy5QC8QQt4t4Wu3p7IvzeneL5I81QjQ1DjMzhbLLorFHgcAs9_FMwnFYFrgsHP1_v3Iqy7zJJc60fCfDaxAF8Txj_LOeOMkCF1-9PwrULWYRTLMI7CdZIm7jb8v9ALxCmDgqUilYvEeBJhgMLezAWtxvGGkejc0BdsbWaPFX1I3Uj7C-Mw8LcmpSLKZyEnhj2x-3Vfv5hIVauC6ja1B6Z_UcqXKOC.N2WVMbpAxiPAtG90.63wRVVKX0ZOxu8cKqN1kqN-7EDa_mnmk32DinS_zFo4.HC7Ev5lmsbTgwyGpeGH5Rw
```

For more detailed examples of this process, check out the sample [Cache-Only Key Wrapper](#) in Github. You can use either the utility in this repository or another service of your choosing.

Configure Your Cache-Only Key Callout Connection

Use a named credential to specify the endpoint for your callout, and identify the key that you want to fetch from your endpoint.

1. Make sure that your org has at least one active Fields and Files (Probabilistic) key, either Salesforce-generated or customer-supplied. You can create a tenant secret by clicking **Generate Tenant Secret** on the Key Management page in Setup.
2. From Setup, in the Quick Find box, enter *Named Credential*, and then select **Named Credential**.

 **Tip:** A named credential provides an authenticated callout mechanism through which Salesforce can fetch your key material. Because named credentials are allowlisted, they're a secure and convenient channel for key material stored outside of Salesforce.

Learn more about named credentials, how to define a named credential, and how to grant access to authentication settings for named credentials in Salesforce Help.

3. Create a named credential. Specify an HTTPS endpoint from which Salesforce can fetch your key material.
4. From Setup, in the Quick Find box, enter *Encryption Settings*, and then select **Encryption Settings**.
5. In the Advanced Encryption Settings section, turn on **Allow Cache-Only Keys**.

You can also enable the Cache-Only Key Service programmatically. For more information, see [EncryptionKeySettings](#) in the *Metadata API Developer Guide*.

 **Note:** If you turn off **Allow Cache-Only Keys**, data that's encrypted with cache-only key material remains encrypted and Salesforce continues to invoke secured callouts. However, you can't modify your cache-only key configuration or add new ones. If you don't want to use cache-only keys, rotate your key material to use customer-supplied (BYOK) key material. Then synchronize all your data, and turn off **Allow Cache-Only Keys**.

6. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Key Management**.
7. In the Key Management Table, select a key type.
8. Click **Bring Your Own Key**.
9. Select a BYOK-compatible certificate from the Choose Certificate dropdown.
10. Select **Use a Cache-Only Key**.
11. For Unique Key Identifier, enter your KID—the unique key identifier for your data encryption key. Your identifier can be a number, a string (2018_data_key), or a UUID (982c375b-f46b-4423-8c2d-4d1a69152a0b).
12. In the Named Credential dropdown, select the named credential associated with your key. You can have multiple keys associated with each named credential.

EDITIONS

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions. Requires purchasing Salesforce Shield or Shield Platform Encryption, and the Cache-Only Key Service.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To create, edit, and delete named credentials:

- Customize Application

To allow cache-only keys with BYOK:

- Customize Application
- AND

Manage Encryption Keys

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:

- Manage Encryption Keys

Manage Certificates

Choose Certificate certificate1 ▾

▼ Certificate Details

Name	certificate1	Unique Name	certificate1
Created Date	3/30/2018 2:05 PM	Expiration Date	3/30/2020 5:00 AM
Key Size	4096		

Upload Key Material Use a Cache-Only Key

Use a Cache-Only Key

Unique Key Identifier my_data_key1| Named Credential Named Credential ▾

Salesforce checks the connection to the endpoint specified by the named credential. If Salesforce can reach the endpoint, the key specified for the Unique Key Identifier becomes the active key. All data marked for encryption by your encryption policy is encrypted with your cache-only key.

If Salesforce can't reach the specified endpoint, an error displays to help you troubleshoot the connection.

Cache-only key status is recorded as Fetched on the Key Management page. In Enterprise API, the TenantSecret `source` value is listed as Remote.

 **Tip:** You can monitor key configuration callouts in the Setup Audit Trail. When a callout to an active or archived cache-only key is successful, the Setup Audit Trail logs an Activated status. Individual callouts aren't monitored in Setup Audit Trail.

SEE ALSO:

[Object Reference for Salesforce and Lightning Platform: RemoteKeyCalloutEvent](#)

Add Replay Detection for Cache-Only Keys

Replay detection protects your cache-only keys if a callout is fraudulently intercepted. When enabled, replay detection inserts an autogenerated, unique marker called a RequestIdentifier into every callout. The RequestIdentifier includes the key identifier, a nonce generated for that callout instance, and the nonce required from the endpoint. The RequestIdentifier serves as a random, one-time identifier for each valid callout request. After you set up your key service to accept and return the RequestIdentifier, any callout with missing or mismatched RequestIdentifiers is aborted.

1. Update your key service to extract the nonce generated for the callout instance from the RequestIdentifier. Here's what the nonce looks like.
e5ab58fd2ced013f2a46d5c8144dd439
2. Echo this nonce in the JWE protected header, along with the algorithm used to encrypt the content encryption key, the algorithm used to encrypt the data encryption key, and the unique ID of the cache-only key. Here's an example.

```
{"alg":"RSA-OAEP","enc":"A256GCM","kid":"982c375b-f46b-4423-8c2d-4d1a69152a0b","jti":"e5ab58fd2ced013f2a46d5c8144dd439"}
```

3. From Setup, in the Quick Find box, enter *Encryption Settings*, and then click **Encryption Settings**.
4. In the Advanced Encryption Settings section, turn on **Enable Replay Detection for Cache-Only Keys**.

You can also enable replay detection programmatically. For more information, see [EncryptionKeySettings](#) in the *Metadata API Developer Guide*.

From now on, every callout to an external key service includes a unique RequestIdentifier.

-  **Warning:** If you enable replay detection but don't return the nonce with your cache-only key material, Salesforce aborts the callout connection and displays a POTENTIAL_REPLAY_ATTACK_DETECTED error.

SEE ALSO:

[Object Reference for Salesforce and Lightning Platform: RemoteKeyCalloutEvent](#)

EDITIONS

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions. Requires purchasing Salesforce Shield or Shield Platform Encryption, and the Cache-Only Key Service.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To create, edit, and delete named credentials:

- Customize Application

To enable replay detection for cache-only keys:

- Customize Application

AND

Manage Encryption Keys

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:

- Manage Encryption Keys

Check Your Cache-Only Key Connection

Because your cache-only key material is stored outside of Salesforce, it's important to maintain a functional callout connection. Use the Callout Check page to monitor your connection and quickly respond to key service interruptions that could prevent the service from fetching your keys.

The Cache-Only Key: Callout Check page is accessible after you enable the Cache-Only Key Service in your org and make your first callout. Data presented as part of a callout check are never stored in the system of record.

1. From Setup, enter *Platform Encryption* in the Quick Find box, then select **Key Management**.
2. Choose the Certificate Unique Name and Named Credential associated with your Unique Key Identifier.
3. In the Actions column, next to the key material you want to check, click **Details**.
4. On the Cache-Only Key: Callout Check page, click **Check**.
Details about your callout connection display on the page. It can take a few moments for the callout check to complete and display the results.

EDITIONS

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions. Requires purchasing Salesforce Shield or Shield Platform Encryption, and the Cache-Only Key Service.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:

- Manage Encryption Keys

Cache-Only Key: Callout Check Help for this Page ?

Review and check your cache-only key callout connection. Callout test results aren't saved or logged in Salesforce.

Callout Connection Details Save Cancel

Unique Key Identifier: keyContact2 Named Credential: Named Credential

Certificate Unique Name: certificate2

Start a callout connection check to see results. Check

Testing callout connection for

Organization ID: 00DR00000013Hj
 Tenant Secret ID: 02GR0000001K1G
 Unique Key Identifier: keyContact2
 Named Credential: Named_Credential
 Certificate Unique Name: certificate2

The callout was successful.

5. Review the details about your callout connection. If your callout connection was unsuccessful, you see a descriptive error message at the bottom of the results pane. Use this message to make the appropriate adjustments to your key service.

SEE ALSO:

[Object Reference for Salesforce and Lightning Platform: RemoteKeyCalloutEvent](#)

Destroy a Cache-Only Key

When you destroy a cache-only key, you're destroying two things: the key in the cache and the callout connection to the key service.

1. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Key Management**.
2. In the Key Management Table, select a key type.
3. Find your key in the table and click **Destroy**.
Your key material's status is changed to Destroyed, and callouts to this key stop. Data encrypted with this key material is masked with "?????" in the app.

 **Note:** Your cache-only key is unique to your org and to the specific data to which it applies. When you destroy a cache-only key, related data isn't accessible unless you reactivate it and make sure that Salesforce can fetch it.

Reactivate a Cache-Only Key

If you still have your named credential associated with a key that was destroyed in Salesforce, you can reactivate a destroyed cache-only key from Setup or programmatically through the API. Reactivating a destroyed key makes it the active key. Before you reactivate a destroyed key, make sure that the corresponding key service connection is recovered.

1. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Key Management**.
2. Find your key in the table and click **Activate**.
The Shield Key Management Service fetches the reactivated cache-only key from your key service and uses it to access data that was previously encrypted with it.

 **Note:** You can sync your data to your active cache-only key just like you can with any other key material.

SEE ALSO:

[Object Reference for Salesforce and Lightning Platform: TenantSecret](#)

EDITIONS

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions. Requires purchasing Salesforce Shield or Shield Platform Encryption, and the Cache-Only Key Service.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:

- Manage Encryption Keys

EDITIONS

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions. Requires purchasing Salesforce Shield or Shield Platform Encryption, and the Cache-Only Key Service.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:

- Manage Encryption Keys

Considerations for Cache-Only Keys

These considerations apply to all data that you encrypt using the Shield Platform Encryption Cache-Only Key Service.

Retry Policy

If Salesforce can't reach your external key service, the callout fails and your active cache-only key's status is set to Destroyed. This policy prevents excessive loads on both services. The Cache-Only Key Service then periodically retries the callout to help you minimize down time. Retries occur one time per minute for five minutes, then one time every five minutes for 24 hours. If the Cache-Only Key Service can successfully complete a callout during this retry period, your cache-only key's status is reset to Active.

At any point during a retry period, you can activate your key material through Setup or the API pending remote key service availability. If you reactivate your key material during the retry period, all retry attempts stop.

The RemoteKeyCalloutEvent object captures every callout to your key service. You can subscribe to this event with after insert Apex triggers, and set up real-time alerts that notify you when a callout fails.

401 HTTP Responses

If there's a 401 HTTP response, Salesforce automatically refreshes any OAuth token associated with your named credential, and retries the request.

CRM Analytics

Backups of CRM Analytics data are encrypted with your Shield Platform Encryption keys. If you encrypt data in CRM Analytics datasets with a cache-only key, make sure that the Analytics cache-only key is in the same state as your Fields and Files (Probabilistic) cache-only key.

Setup Audit Trail

Setup Audit Trail records activated cache-only key versions differently depending on whether a cache-only key with the Active status exists when you reactivate the key.

However, if you reactivate a destroyed key and there's already another key with the Active status, the Setup Audit Trail shows the reactivated key with an updated version number.

Cache-Only Keys and Key Types

Use a separate cache-only key for each type of data you want to encrypt. You can't use a cache-only key with multiple key types. For example, you can't use a cache-only key to encrypt both search indexes and CRM Analytics data.

Service Protections

To protect against Shield KMS interruptions and ensure smooth encryption and decryption processes, you can have up to 10 active and archived cache-only keys of each type.

If you reach your key limit, destroy an existing key so that you can create, upload, reactivate, rearchive, or create a callout to another one. Remember to synchronize your data with an active key before destroying key material.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Troubleshoot Cache-Only Keys

One or more of these frequently asked questions may help you troubleshoot any problems that arise with Shield Platform Encryption's Cache-Only Key Service.

The callout to my key service isn't going through. What can I do?

Callouts can fail for various reasons. Review the error message that displays and follow these tips for resolving the problem. All callouts are recorded in the [RemoteKeyCalloutEvent](#) object.

Table 9: Cache-Only Key Service Errors and Status Codes

RemoteKeyCalloutEvent Status Code	Error	Tips for Fixing the Problem
DESTROY_HTTP_CODE	The remote key service returned an HTTP error: {000}. A successful HTTP response returns a 200 code.	To find out what went wrong, review the HTTP response code.
ERROR_HTTP_CODE	The remote key service returned an unsupported HTTP response code: {000}. A successful HTTP response returns a 200 code.	To find out what went wrong, review the HTTP response code.
MALFORMED_CONTENT_ENCRYPTION_KEY	The remote key service returned a content encryption key in the JWE that couldn't be decrypted with the certificate's private key. Either the JWE is corrupted, or the content encryption key is encrypted with a different key.	Check that you set up your named credential properly and are using the correct BYOK-compatible certificate.
MALFORMED_DATA_ENCRYPTION_KEY	The content encryption key couldn't decrypt the data encryption key that was returned in the remote key service's JWE. The data encryption key is either malformed, or encrypted with a different content encryption key.	Check that you set up your named credential properly and are using the correct BYOK-compatible certificate. Named credentials must call out to an HTTPS endpoint.
MALFORMED_JSON_RESPONSE	We can't parse the JSON returned by your remote key service. Contact your remote key service for help.	Contact your remote key service.
MALFORMED_JWE_RESPONSE	The remote key service returned a malformed JWE token that can't be decoded. Contact your remote key service for help.	Contact your remote key service.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

RemoteKeyCalloutEvent Status Code	Error	Tips for Fixing the Problem
EMPTY_RESPONSE	The remote key service callout returned an empty response. Contact your remote key service for help.	Contact your remote key service.
RESPONSE_TIMEOUT	The remote key service callout took too long and timed out. Try again.	If your key service is unavailable after multiple callout attempts, contact your remote key service.
UNKNOWN_ERROR	The remote key service callout failed and returned an error: {000}.	Contact your remote key service.
INCORRECT_KEYID_IN_JSON	The remote key service returned JSON with an incorrect key ID. Expected: {valid keyID}. Actual: {invalid keyID}.	Check that you set up your named credential properly and are using the correct BYOK-compatible certificate.
INCORRECT_KEYID_IN_JWE_HEADER	The remote key service returned a JWE header with an incorrect key ID. Expected: {valid keyID}. Actual: {invalid keyID}.	Check that you set up your named credential properly and are using the correct BYOK-compatible certificate.
INCORRECT_ALGORITHM_IN_JWE_HEADER	The remote key service returned a JWE header that specified an unsupported algorithm (alg): {algorithm}.	The algorithm for encrypting the content encryption key in your JWE header must be in RSA-OAEP format.
INCORRECT_ENCRYPTION_ALGORITHM_IN_JWE_HEADER	The remote key service returned a JWE header that specified an unsupported encryption algorithm (enc): {your enc}.	The algorithm for encrypting the data encryption key in your JWE header must be in A256GCM format.
INCORRECT_DATA_ENCRYPTION_KEY_SIZE	Data encryption keys encoded in a JWE must be 32 bytes. Yours is {value} bytes.	Make sure that your data encryption key is 32 bytes.
ILLEGAL_PARAMETERS_IN_JWE_HEADER	Your JWE header must use {0}, but no others. Found: {1}.	Remove the unsupported parameters from your JWE header.
MISSING_PARAMETERS_IN_JWE_HEADER	Your JWE header is missing one or more parameters. Required: {0}. Found:{1}.	Make sure that your JWE header includes all required values. For example, if Replay Detection is enabled, the JWE header must include the nonce value extracted from the cache-only key callout.
AUTHENTICATION_FAILURE_RESPONSE	Authentication with the remote key service failed with the following error: {error}.	Check the authentication settings for your chosen named credential.
POTENTIAL_REPLAY_ATTACK_DETECTED	The remote key service returned a JWE header with an incorrect nonce value. Expected: {0}. Actual: {1}	Make sure that your JWE header includes the RequestID included in the callout.
UNKNOWN_ERROR	The remote key service callout failed and returned an error: java.security.cert.CertificateExpiredException: NotAfter: {date and time of expiration}	The certificate for your cache-only key expired. Update your cache-only key material to use an active BYOK-compatible certificate.

The following key service errors can prevent the callout from completing. If you see errors related to these problems, contact your key service administrator for help.

- The JWE is corrupt or malformed.
- The data encryption key is malformed.
- The key service returned a malformed JWE token.
- The key service returned an empty response.

For uniform resource use, Salesforce limits the amount of time for each key service callout to 3 seconds. If the callout takes more than the allotted time, Salesforce fails the callout with a timeout error. Check that your key service is available. Make sure that your named credential references the correct endpoint—check the URL, including the IP address.

Can I execute a remote callout in Apex?

Yes. Salesforce manages all authentication for Apex callouts that specify a named credential as the callout endpoint so that your code doesn't have to. To reference a named credential from a callout definition, use the named credential URL. A named credential URL contains the scheme callout, the name of the named credential, and an optional path. For example:
callout:My_Named_Credential/some_path.

See [Named Credentials as Callout Endpoints](#) in the Apex Developer Guide.

Can I monitor my callout history?

If you want to review or track cache-only key events, use the RemoteKeyCalloutEvent standard object. Either use the `describeSObjects()` call to view event information, or an after insert Apex trigger to perform custom actions after each callout. For example, you can write a trigger that stores RemoteKeyCallout events in a custom object. When you store RemoteKeyCallout events in a custom object, you can monitor your callout history. See the [RemoteKeyCalloutEvent](#) entry in the *Salesforce Object Reference* for more information.

The Setup Audit Trail tracks changes in key material state and named credential settings. Callout history isn't recorded in log files.

When I try to access data encrypted with a cache-only key, I see "?????" instead of my data. Why?

Masking means one of two things. Either the connection to your key service is broken and we can't fetch your key, or the data is encrypted with a destroyed key. Check that your key service is available and that your named credential references the correct endpoint. If any key versions are marked as Destroyed as a result of a key service failure, recover the connection and manually activate the key version.

Do I have to make a new named credential every time I rotate a key?

Nope. You can use a named credential with multiple keys. As long as you host your key material at the endpoint specified in an existing named credential, you're all set. When you rotate your key material, change the key ID in the Unique Key Identifier field. Double-check that your new key is stored at the specified endpoint URL in your named credential.

I'm still having problems with my key. Who should I talk to?

If you still have questions, contact your account executive or Salesforce Customer Support. They'll put you in touch with a support team specific to this feature.

SEE ALSO:

[Object Reference for Salesforce and Lightning Platform: RemoteKeyCalloutEvent Key Management and Rotation](#)

Shield Platform Encryption Customizations

Some features and settings require adjustment before they work with encrypted data.

[Apply Encryption to Fields Used in Matching Rules](#)

Matching rules used in duplicate management help you maintain clean and accurate data. To make fields encrypted with Shield Platform Encryption compatible with standard and custom matching rules, use the deterministic encryption scheme.

[Use Encrypted Data in Formulas](#)

Use custom formula fields to quickly find encrypted data. Shield Platform Encryption is compatible with several operators and functions, and can render encrypted data in text, date, and date/time formats, and reference quick actions.

SEE ALSO:

[Strengthen Your Data's Security with Shield Platform Encryption](#)

Apply Encryption to Fields Used in Matching Rules

Matching rules used in duplicate management help you maintain clean and accurate data. To make fields encrypted with Shield Platform Encryption compatible with standard and custom matching rules, use the deterministic encryption scheme.

Before you start, turn on **Deterministic Encryption** from the Encryption Settings page. If you don't have a Fields (Deterministic) type tenant secret, create one from the Key Management page.

! **Important:** Matching rules used in duplicate management don't support probabilistically encrypted data.

Follow these steps to add encrypted fields to existing custom matching rules.

1. From Setup, in the Quick Find box, enter *Matching Rules*, and then select **Matching Rules**.
2. Deactivate the matching rule that reference fields that you want to encrypt. If your matching rule is associated with an active duplicate rule, first deactivate the duplicate rule from the Duplicate Rules page. Then return to the Matching Rules page and deactivate the matching rule.
3. From Setup, in the Quick Find box, enter *Encryption Settings*, and then select **Encryption Settings**.
4. In the Advanced Encryption Settings section, click **Select Fields**.
5. Click **Edit**.
6. Select the fields that you want to encrypt, and select **Deterministic** from the Encryption Scheme list.



EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:

- View Setup and Configuration

To enable encryption key (tenant secret) management:

- Manage Profiles and Permission Sets

7. Save your work.

 **Tip:** Standard matching rules are automatically deactivated when encryption is added to a field referenced by that rule. To encrypt fields referenced in standard matching rules, follow steps 3–8.

8. After you get the email verifying encryption's been enabled on your fields, reactivate your matching rule and associated duplicate management rule.

Matching rules used in duplicate management now return exact and fuzzy matches on encrypted data.

 **Example:** Let's say that you encrypted the Billing Address on your Contacts, and you want to add this field to a custom matching rule. First, deactivate the rule or rules that you want to add this field to. Make sure that the Billing Address field is encrypted with the deterministic encryption scheme. Then add Billing Address to your custom matching rule, just like how you add any other field. Finally, reactivate your rule.

When you rotate your key material, you must update custom matching rules that reference encrypted fields. After you rotate your key material, deactivate and then reactivate the affected matching rules. Then contact Salesforce to request the background encryption process. When the background encryption process finishes, your matching rules can access all data encrypted with your active key material.

 **Important:** To ensure accurate matching results, customers who used the beta version of this feature must deactivate any matching rules that reference encrypted fields and then reactivate them. If your custom matching rule fails on reactivation, contact Salesforce for help with reactivating your match index.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

Use Encrypted Data in Formulas

Use custom formula fields to quickly find encrypted data. Shield Platform Encryption is compatible with several operators and functions, and can render encrypted data in text, date, and date/time formats, and reference quick actions.

Supported Operators, Functions, and Actions

Supported operators and functions:

- & and + (concatenate)
- BLANKVALUE
- CASE
- HYPERLINK
- IF
- IMAGE
- ISBLANK
- ISNULL
- NULLVALUE

Also supported:

- Spanning
- Quick actions

Formulas can return data only in `text`, `date`, or `date/time` formats.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

& and + (Concatenate)**This works:**

```
(encryptedField__c & encryptedField__c)
```

Why it works:

This formula works because & is supported.

This doesn't work:

```
LOWER(encryptedField__c & encryptedField__c)
```

Why it doesn't work:

LOWER isn't a supported function, and the input is an encrypted value.

Case

CASE returns encrypted field values, but doesn't compare them.

This works:

```
CASE(custom_field__c, "1", cf2__c, cf3__c)
```

where either or both cf2__c and cf3__c are encrypted

Why it works:

custom_field__c is compared to "1". If it's true, the formula returns cf2__c because it's not comparing two encrypted values.

This doesn't work:

```
CASE("1", cf1__c, cf2__c, cf3__c)
```

where cf1__c is encrypted

Why it doesn't work:

You can't compare encrypted values.

ISBLANK and ISNULL**This works:**

```
OR(ISBLANK(encryptedField__c), ISNULL(encryptedField__c))
```

Why it works:

Both ISBLANK and ISNULL are supported. OR works in this example because ISBLANK and ISNULL return a Boolean value, not an encrypted value.

Spanning**This works:**

```
(LookupObject1__r.City & LookupObject1__r.Street) &
(LookupObject2__r.City & LookupObject2__r.Street) &
(LookupObject3__r.City & LookupObject3__r.Street) &
(LookupObject4__r.City & LookupObject4__r.Street)
```

How and why you use it:

Spanning retrieves encrypted data from multiple entities. For example, let's say you work in the customer service department for Universal Containers. A customer has filed a case about a distribution problem, and you want to see the scope of the issue. You want all the shipping addresses related to this particular case. This example returns all the customers' shipping addresses as a single string in your case layout.

Validation

The encryption validation service checks your org to make sure that it's compatible with encrypted formula field types.

When you encrypt a given field, the validation service:

- Retrieves all formula fields that reference the field
- Verifies that the formula fields are compatible with encryption
- Verifies that the formula fields aren't used elsewhere for filtering or sorting

Limits

Up to 200 formula fields can reference a given encrypted custom field. A field that is referenced by more than 200 formula fields can't be encrypted. If you must reference an encrypted custom field from more than 200 formula fields, contact Salesforce.

When you specify multiple fields to encrypt at one time, the 200-field limit is applied to the whole batch. If you know that you're encrypting fields that have multiple formula fields pointing to them, encrypt those fields one at a time.

SEE ALSO:

[General Shield Platform Encryption Considerations](#)

Tradeoffs and Limitations of Shield Platform Encryption

A security solution as powerful as Shield Platform Encryption doesn't come without some tradeoffs. When your data is encrypted, some users may see limitations to some functionality, and a few features aren't available at all. Consider the impact on your users and your overall business solution as you design your encryption strategy.

[Shield Platform Encryption Best Practices](#)

Take the time to identify the most likely threats to your org. This process helps you distinguish data that needs encryption from data that doesn't, so that you can encrypt only what you need to. Make sure that your tenant secret and keys are backed up, and be careful who you allow to manage your secrets and keys.

[General Shield Platform Encryption Considerations](#)

These considerations apply to all data that you encrypt using Shield Platform Encryption.

[Considerations for Using Deterministic Encryption](#)

These considerations apply to data encrypted with Shield Platform Encryption's deterministic encryption scheme. Some considerations manifest differently depending on whether data is encrypted with the case-sensitive or case-insensitive deterministic encryption scheme.

[Shield Platform Encryption and the Lightning Experience](#)

Shield Platform Encryption works the same way in the Lightning Experience as it does in Salesforce Classic, with a few minor exceptions.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

[Field Limits with Shield Platform Encryption](#)

Under certain conditions, encrypting a field can impose limits on the values that you store in that field. If you expect users to enter non-ASCII values, such as Chinese, Japanese, or Korean-encoded data, we recommend creating validation rules to enforce these field limits.

[Which Salesforce Apps Don't Support Shield Platform Encryption?](#)

Some Salesforce features work as expected when you work with data that's encrypted with Shield Platform Encryption. Others don't.

SEE ALSO:

[Strengthen Your Data's Security with Shield Platform Encryption](#)

Shield Platform Encryption Best Practices

Take the time to identify the most likely threats to your org. This process helps you distinguish data that needs encryption from data that doesn't, so that you can encrypt only what you need to. Make sure that your tenant secret and keys are backed up, and be careful who you allow to manage your secrets and keys.

1. Define a threat model for your organization.

To identify the threats that are most likely to affect your organization, walk through a formal threat modeling exercise. Use your findings to create a data classification scheme, which can help you decide what data to encrypt.

2. Encrypt only where necessary.

- Not all data is sensitive. Focus on information that requires encryption to meet your regulatory, security, compliance, and privacy requirements. Unnecessarily encrypting data impacts functionality and performance.
- Evaluate your data classification scheme early and work with stakeholders in security, compliance, and business IT departments to define requirements. Balance business-critical functionality against security and risk measures and challenge your assumptions periodically.

3. Create a strategy early for backing up and archiving keys and data.

If your tenant secrets are destroyed, reimport them to access your data. You are solely responsible for making sure that your data and tenant secrets are backed up and stored in a safe place. Salesforce cannot help you with deleted, destroyed, or misplaced tenant secrets.

4. Read the Shield Platform Encryption considerations and understand their implications on your organization.

- Evaluate the impact of the considerations on your business solution and implementation.
- Test Shield Platform Encryption in a sandbox environment before deploying to a production environment. Encryption policy settings can be deployed using change sets.
- Before enabling encryption, fix any violations that you uncover. For example, if you reference encrypted fields in a SOQL ORDER BY clause, a violation occurs. Fix the violation by removing references to the encrypted fields.
- When requesting feature enablement, such as pilot features, give Salesforce Customer Support several days lead time. The time to complete the process varies based on the feature and how your org is configured.

5. Analyze and test AppExchange apps before deploying them.

- If you use an app from the AppExchange, test how it interacts with encrypted data in your organization and evaluate whether its functionality is affected.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

- If an app interacts with encrypted data that's stored outside of Salesforce, investigate how and where data processing occurs and how information is protected.
- If you suspect Shield Platform Encryption could affect the functionality of an app, ask the provider for help with evaluation. Also discuss any custom solutions that must be compatible with Shield Platform Encryption.
- Apps on the AppExchange that are built exclusively using Lightning Platform inherit Shield Platform Encryption capabilities and limitations.

6. Use out-of-the-box security tools.

Shield Platform Encryption is not a user authentication or authorization tool. To control which users can see which data, use out-of-the-box tools such as field-level security settings, page layout settings, and sharing rules, rather than Shield Platform Encryption.

7. Grant the Manage Encryption Keys user permission to authorized users only.

Users with the Manage Encryption Keys permission can generate, export, import, and destroy organization-specific keys. Monitor the key management activities of these users regularly with the setup audit trail.

8. Synchronize your existing data with your active key material.

Existing field and file data is not automatically encrypted when you turn on Shield Platform Encryption. To encrypt existing field data, update the records associated with the field data. This action triggers encryption for these records so that your existing data is encrypted at rest. To encrypt existing files or get help updating other encrypted data, contact Salesforce. We can encrypt existing file data in the background to ensure data alignment with the latest encryption policy and key material.

When you contact Salesforce support to request the background encryption service, allow at least a week before you need the background encryption completed. The time to complete the process varies based on the volume of data involved. It could take several days.

9. Handle currency and number data with care.

Currency and Number fields can't be encrypted because they could have broad functional consequences across the platform, such as disruptions to roll-up summary reports, report timeframes, and calculations. You can often keep private, sensitive, or regulated data of this variety safe in other encryption-supported field types.

10. Communicate to your users about the impact of encryption.

Before you enable Shield Platform Encryption in a production environment, inform users about how it affects your business solution. For example, share the information described in Shield Platform Encryption considerations, where it's relevant to your business processes.

11. Encrypt your data using the most current key.

When you generate a new tenant secret, any new data is encrypted using this key. However, existing sensitive data remains encrypted using previous keys. In this situation, Salesforce strongly recommends re-encrypting these fields using the latest key. Contact Salesforce for help with re-encrypting your data.

12. Use discretion when granting login as access to users or Salesforce Customer Support.

If you grant login access to a user, and they have field level security access to an encrypted field, that user is able to view encrypted data in that field in plaintext.

If you want Salesforce Customer Support to follow specific processes around asking for or using login as access, you can create special handling instructions. Salesforce Customer Support follows these instructions in situations where login as access may help them resolve your case. To set up these special handling instructions, contact your account executive.

General Shield Platform Encryption Considerations

These considerations apply to all data that you encrypt using Shield Platform Encryption.

Important: Where possible, we changed noninclusive terms to align with our company value of Equality. We maintained certain terms to avoid any effect on customer implementations.

Leads

Lead and Case assignment rules, workflow rules, and validation rules work normally when Lead fields are encrypted. Matching and de-duplication of records during lead import works with deterministic encryption but not probabilistic encryption. Einstein Lead Scoring isn't available.

Apex Lead Conversion works normally, but PL-SQL-based lead conversion isn't supported.

User Email

Many Salesforce features rely on the User Email field. Most work seamlessly with Shield Platform Encryption. But the following products and features behave differently when User Email is encrypted.

- User Email is unencrypted when Lightning Sync or Einstein Activity Capture are enabled. Lightning Sync and Einstein Activity Capture duplicate the User Email field in the database when users are added to sync configurations for those products. Even if you encrypt the User Email field with Shield Platform Encryption, this duplicate field stores user emails in the Salesforce database in an unencrypted state. For more information, see [Considerations for Syncing Contacts](#), [Considerations for Syncing Events](#), and [Considerations for Setting Up Einstein Activity Capture](#).
- Event functionality that relies on user emails, especially calendar invitations, can be interrupted. Before encrypting the User Email field in production environments, Salesforce recommends that you test Activity features in a sandbox.
- You can't sort records in list views by fields that contain encrypted data. If you encrypt User email, you can't add it as a filter in reports.
- Login Discovery Handler lookups that rely on emails don't work if the email field is encrypted, which can block user logins. If your lookups rely on emails, don't encrypt the User Email field.
- If you use Einstein Conversation Insights, encrypt User Email with case-insensitive deterministic encryption. Some Einstein Conversation Insights features, including video calls, don't work when User Email is encrypted with probabilistic encryption.

Flows and Processes

You can reference encrypted fields in most places in your flows and processes. However, you can't reference encrypted fields in these filtering or sorting contexts.

Tool	Filtering Availability	Sorting Availability
Process Builder	Update Records action	n/a
Flow Builder	Record Choice Set resource Get Records element Delete Records element Update Records element Condition requirements	Record Choice Set resource Get Records element

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

You can store the value from an encrypted field in a variable and operate on that value in your flow's logic. You can also update the value for an encrypted field.

Paused flow interviews can cause data to be saved in an unencrypted state. When a flow or process is waiting to resume, the associated flow interview is serialized and saved to the database. The flow interview is serialized and saved when:

- Users pause a flow
- Flows execute a Wait element
- Processes are waiting to execute scheduled actions

If the flow or process loads encrypted fields into a variable during these processes, that data isn't always encrypted at rest.

Next Best Action Recommendations

When you use probabilistic encryption, you can't use encrypted fields like Recommendation Description when you specify conditions to load recommendations.

Custom Fields

You can't use encrypted custom fields in criteria-based sharing rules.

Some custom fields can't be encrypted.

- Fields that have the `Unique` or `External ID` attributes or include these attributes on previously encrypted custom fields (applies only to fields that use the probabilistic encryption scheme)
- Fields on external data objects
- Fields that are used in an account contact relation

You can't use Schema Builder to create an encrypted custom field.

You can't use Shield Platform Encryption with Custom Metadata Types.

SOQL and SOSL

- You can't include fields encrypted with the probabilistic encryption scheme in the following SOQL and SOSL clauses and functions:
 - Aggregate functions such as `MAX()`, `MIN()`, and `COUNT_DISTINCT()`
 - WHERE clause
 - GROUP BY clause
 - ORDER BY clause

For information about SOQL and SOSL compatibility with deterministic encryption, see [Considerations for Using Deterministic Encryption in Salesforce Help](#).



Tip: Consider whether you can replace a WHERE clause in a SOQL query with a FIND query in SOSL.

- When you query encrypted data, invalid strings return an `INVALID_FIELD` error instead of the expected `MALFORMED_QUERY`.

Marketing Cloud Account Engagement

Account Engagement supports contact email addresses encrypted by Shield Platform Encryption as long as your instance meets a few conditions. Your org must allow multiple prospects with the same email address. After this feature is enabled, you can add the contact email address field to your encryption policy.

Because the contact email address shows in the Permission object, users must have permission to view the Prospect object.

If you encrypt the contact email address field, the Salesforce Connector can't use the email address as a secondary prospect match criteria. For more information, read [Salesforce Connector Settings](#).

Portals

If a legacy portal (created before 2013) is enabled in your org, you can't encrypt standard fields. Deactivate all legacy customer and partner portals to enable encryption on standard fields. (Salesforce Experience Cloud sites are supported.)

To deactivate a legacy customer portal, go to the Customer Portal Settings page in Setup. To deactivate a legacy partner portal, go to the Partners page in Setup.

Salesforce B2B Commerce

Shield Platform Encryption supports version 4.10 and later of the Salesforce B2B Commerce managed package, with some behavior differences. For a complete list of considerations, see [Enable Shield Platform Encryption for B2B Commerce for Visualforce Objects](#).

Search

If you encrypt fields with a key and then destroy the key, the corresponding search terms remain in the search index. However, you can't decrypt the data associated with the destroyed key.

Accounts, Person Accounts, and Contacts

When Person Accounts are turned on, encrypting any of the following Account fields encrypts the equivalent Contact fields, and vice versa.

- Name
- Description
- Phone
- Fax

When you encrypt any of the following Account or Contact fields, the equivalent fields in Person Accounts are also encrypted.

- Name
- Description
- Mailing Address
- Phone
- Fax
- Mobile
- Home Phone
- Other Phone
- Email

When the Account Name or Contact Name field is encrypted, searching for duplicate accounts or contacts to merge doesn't return any results.

When you encrypt the First Name or Last Name field on a contact, that contact appears in the Calendar Invite lookup only if you haven't filtered by First Name or Last Name.

Email Bounce Handling

Bounce handling doesn't support encrypted email addresses. If you need email bounce handling, don't encrypt the standard Email field.

Email-to-Case

Copying text from email fields also copies unicode characters embedded in email text. Two of those unicode character sequences, `\uFFFF` and `\uFFFF`, can't be included in text encrypted by Shield Platform Encryption. If you encounter an error mentioning these unicode sequences, delete the text copied from the email field and type it manually.

Activity Subject and Description

You can encrypt an Activity Subject field with case-insensitive encryption. If you destroy key material that encrypts a field, filtering on the field doesn't yield matches.

If you encrypt the Activity Subject field and it's used in a custom picklist, delete and replace actions aren't available for that value. To remove an Activity Subject value from a picklist, deactivate it.

Activity Subject fields that include an OrgID aren't copied over when you create a sandbox copy of a production org.

Encrypting Activity Description also encrypts the Task Comment field. The validation email lists the Task Comment field but not Activity Description, even though both fields are encrypted.

Salesforce for Outlook

If you encrypt the same fields that you filter in Salesforce for Outlook data sets, Salesforce for Outlook doesn't sync. To get Salesforce for Outlook to sync again, remove the encrypted fields from your filters in your data sets.

Campaigns

Campaign member search isn't supported when you search by encrypted fields.

Notes

You can encrypt the body text of Notes created with the new Notes tool. However, the Preview file and Notes created with the old Notes tool aren't supported.

Field Audit Trail

Data in a previously archived Field Audit Trail isn't encrypted when you turn on Platform Encryption. For example, say that your org uses Field Audit Trail to define a data history retention policy for an account field, such as the phone number field. When you turn on encryption for that field, new phone number records are encrypted as they're created. Previous updates to the phone number field that are stored in the Account History related list are also encrypted. However, phone number history data that is already archived in the `FieldHistoryArchive` object is stored without encryption. To encrypt previously archived data, contact Salesforce.

Salesforce Experiences

If you encrypt the Account Name field and you're not using Person Accounts, encryption affects how users' roles are displayed to admins. Normally, a site user's role name is displayed as a combination of their account name and the name of their user profile. When you encrypt the Account Name field, the account ID is displayed instead of the account name.

For example, when the Account Name field isn't encrypted, users belonging to the Acme account with the Customer User profile would have a role called `Acme Customer User`. When Account Name is encrypted (and Person Accounts aren't in use), the role is displayed as something like `001D000000IRt53 Customer User`.

Data Import Wizard

You can't use the Data Import Wizard to perform matching using master-detail relationships or update records that contain fields that use the probabilistic encryption scheme. You can use it to add new records, however.

Reports, Dashboards, and List Views

- Report charts and dashboard components that display encrypted field values might be cached unencrypted.
- You can't sort records in list views by fields that contain encrypted data.

Encryption for Chatter

When you embed a custom component in your Chatter feed using Rich Publisher Add-Ons, the data related to those add-ons is encoded, but it isn't encrypted with the Shield Platform Encryption service. Unencrypted data in Rich Publisher Add-Ons includes data stored in the Extension ID, Text Representation, Thumbnail URL, Title, Payload, and PayloadVersion fields.

Encryption for Custom Matching Rules Used in Duplicate Management

Custom matching rules can only reference fields encrypted with the deterministic encryption scheme. Probabilistic encryption isn't supported. When you rotate your keys, you must deactivate and then reactivate custom matching rules that reference encrypted fields. If you don't take this step after updating your key material, matching rules don't find all your encrypted data.

Standard matching rules that include fields with Shield Platform Encryption don't detect duplicates. If you encrypt a field included in standard matching rules, deactivate the standard rule.

Service protections ensure that loads are balanced across the system. The matching service searches for match candidates until it finds all matches up to 200 matches. With Shield Platform Encryption, the service search maximum is 100 candidates. With encryption, you could find fewer or no possible duplicate records.

Duplicate jobs aren't supported.

Self-Service Background Encryption

Self-service background encryption can encrypt data once every 7 days. This limit includes synchronization processes initiated from the Encryption Statistics and Data Sync page, synchronization that automatically runs when you disable encryption on a field, and synchronization completed by Salesforce Customer Support at your request.

Some conditions prevent the self-service background encryption from running:

- There are more than 10 million records in an object
- The org has destroyed key material
- An object's data is already synchronized
- The synchronization process is already running, initiated either by the customer or by Salesforce Customer Support at the customer's request
- Statistics are being gathered
- An encryption policy change is being processed, such as enabling encryption on a field or data element

After you begin the synchronization processes, wait until it finishes before changing your encryption policy or generating, uploading, or deleting key material. These actions abort the synchronization process.

Employees

If the email field is encrypted using probabilistic encryption, wellness check surveys can't be used. Deterministic encryption is fully supported.

Messaging End User

Encrypting fields on the Messaging End User object sometimes affects indexing. If you see performance degradation on these fields, manually create custom indexes on the affected fields after enabling encryption.

General

- Encrypted fields can't be used in:
 - Criteria-based sharing rules
 - Similar opportunities searches
 - External lookup relationships
- Fields encrypted with the probabilistic encryption scheme can't be used in filter criteria for data management tools. For considerations specific to filter-preserving deterministic encryption, read [Considerations for Using Deterministic Encryption](#).
- Web-to-Case is supported, but the Web Company, Web Email, Web Name, and Web Phone fields aren't encrypted at rest.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

Considerations for Using Deterministic Encryption

These considerations apply to data encrypted with Shield Platform Encryption's deterministic encryption scheme. Some considerations manifest differently depending on whether data is encrypted with the case-sensitive or case-insensitive deterministic encryption scheme.

Key Rotation and Filter Availability

When you rotate key material or change a field's encryption scheme to case-sensitive deterministic encryption or case-insensitive deterministic encryption, synchronize your data. Syncing applies the active Fields (Deterministic) key material to existing and new data. If you don't sync your data, filtering and queries on fields with unique attributes don't return accurate results.

You can sync most data yourself from the Encryption Statistics and Data Sync page in Setup. See [Synchronize Your Data Encryption with the Background Encryption Service](#).

Available Fields and Other Data

Deterministic encryption is available for custom URL, email, phone, text, and text area field types. It isn't available for the following types of data:

- Custom date, date/time, long text area, rich text area, or description field types
- Chatter
- Files and attachments

Filter Operators

In reports and list views, the operators "equals" and "not equal to" are supported with case-sensitive deterministic encryption. Other operators, like "contains" or "starts with," don't return an exact match and aren't supported. Features that rely on unsupported operators, such as Refine By filters, also aren't supported.

Case-insensitive deterministic encryption supports list views and reports. However, the user interface displays all operators, including operators that aren't supported for encrypted data. To review the list of supported operators, see [Use Encrypted Data in Formulas](#).

Formulas

Fields encrypted with the deterministic encryption scheme can't be referenced in SOQL WHERE queries.

Case Sensitivity

When you use case-sensitive deterministic encryption, case matters. In reports, list views, and SOQL queries on encrypted fields, the results are case-sensitive. Therefore, a SOQL query against the Contact object, where LastName = Jones, returns only Jones, not jones or JONES. Similarly, when the case-sensitive deterministic scheme tests for unicity (uniqueness), each version of "Jones" is unique.

Custom Field Allocations

To allow case-insensitive queries, Salesforce stores a lowercase duplicate of your data as a custom field in the database. These duplicates are necessary to enable case-insensitive queries, but they count against your total custom field count.

API Options to Identify Filterable Fields

Fields encrypted using the deterministic encryption scheme are filterable. You can use the `isFilterable()` method to determine the encryption scheme of a particular encrypted field. If the field is filterable, the method returns true.

However, you can't explicitly detect or set the deterministic encryption scheme via the API.

External ID

Case-insensitive deterministic encryption supports Text and Email external ID custom fields but not other external ID custom fields. When you create or edit these fields, use one of the following field setting combinations.

External ID Field Type	Unique Attributes	Encrypted
Text	None	Use case-insensitive deterministic encryption
Text	Unique and case sensitive	Use case-sensitive deterministic encryption
Text	Unique and case insensitive	Use case-insensitive deterministic encryption
Email	None	Use case-insensitive deterministic encryption
Email	Unique	Use case-sensitive deterministic encryption

You can't save changes to both Unique - Case-Sensitive and Encrypted options at the same time. Change one setting, save it, then change the next.

Compound Fields

Even with deterministic encryption, some kinds of searches don't work when data is encrypted with case-sensitive deterministic encryption. Concatenated values, such as compound names, aren't the same as the separate values. For example, the ciphertext for the compound name "William Jones" isn't the same as the concatenation of the ciphertexts for "William" and "Jones".

So, if the First Name and Last Name fields are encrypted in the Contacts object, this query doesn't work:

```
Select Id from Contact Where Name = 'William Jones'
```

But this query does work:

```
Select Id from Contact Where FirstName = 'William' And LastName ='Jones'
```

Case-sensitive and case-insensitive deterministic encryption schemes support compound fields, but only with individual column queries.

Filter Records by Strings

You can search for records using strings. However, commas in strings act as OR statements. If your string includes a comma, use quotation marks around the string. For example, a search for "Universal Containers, Inc, Berlin" returns records that include the full string, including the comma. Searches for *Universal Containers, Inc, Berlin* returns records that include "Universal Containers" or "Inc" or "Berlin".

SOQL GROUP BY Statements

You can use most of the SOQL statements with deterministic encryption. One exception is GROUP BY, which isn't supported, even though you can group report results by row or column.

SOQL LIKE and STARTS WITH Statements

Deterministic encryption only supports exact, case-sensitive matches. Comparison operators that return partial matches aren't supported. For example, LIKE and STARTS WITH statements aren't supported.

SOQL ORDER BY Statements

Because deterministic encryption doesn't maintain the sort order of encrypted data in the database, ORDER BY isn't supported.

Indexes

Case-sensitive deterministic encryption supports single-column indexes, single-column case-sensitive unique indexes, two-column indexes, and custom indexes on standard and custom fields.

Case-insensitive deterministic encryption offers limited support for standard indexes on the following standard fields.

- Contact—Email
- Email Message—Relation
- Lead—Email
- Name

Queries against these fields, when encrypted with case-insensitive deterministic encryption, can perform poorly with large tables. For optimal query performance, use custom indexes instead of standard indexes. To set up custom indexes, contact Salesforce Customer Support.

Expect the enablement process to take longer when you apply deterministic encryption to a field with a large number of records. To support filtering, the enablement process also rebuilds field indexes.

Next Best Action Recommendations

When you use deterministic encryption, you can use encrypted fields in load conditions only with the equals or not equals operator.

Chat

For the best possible recommendation results, use the case-sensitive deterministic encryption scheme with the Utterance field on the Utterance Suggestion object. This field doesn't support other encryption schemes at this time.

The Actor Name field on the Conversation Entry object supports case-sensitive deterministic encryption, but not case-insensitive deterministic encryption.

Converting Account and Contact Records to Person Accounts

When you convert account and contact records to Person Accounts, synchronize your data. Syncing resets the indexes that allow case-insensitive filtering.

Shield Platform Encryption and the Lightning Experience

Shield Platform Encryption works the same way in the Lightning Experience as it does in Salesforce Classic, with a few minor exceptions.

Notes

Note previews in Lightning are not encrypted.

File Encryption Icon

The icon that indicates that a file is encrypted doesn't appear in Lightning.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Field Limits with Shield Platform Encryption

Under certain conditions, encrypting a field can impose limits on the values that you store in that field. If you expect users to enter non-ASCII values, such as Chinese, Japanese, or Korean-encoded data, we recommend creating validation rules to enforce these field limits.

	API Length	Byte Length	Non-ASCII Characters
Assistant Name (Contact)	40	120	22
Address (To, CC, BCC on Email Message) (when encrypted with probabilistic or case-sensitive deterministic encryption)	2959	4000	1333
City (Account, Contact, Lead)	40	120	22
Email (Contact, Lead)	80	240	70
Fax (Account)	40	120	22
First Name (Account, Contact, Lead)	40	120	22
Last Name (Contact, Lead)	80	240	70
Middle Name (Account, Contact, Lead)	40	120	22
Name (Custom Object)	80	240	70
Name (Opportunity)	120	360	110
Phone (Account, Contact)	40	120	22
Site (Account)	80	240	70
Subject (Email Message)(when encrypted with probabilistic or case-sensitive deterministic encryption)	2207	3000	1000
Title (Contact, Lead)	128	384	126

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.



Note: This list isn't exhaustive. For information about a field not shown here, refer to the API.

Email Message Fields and Case-Insensitive Encryption

To encrypt Address and Subject fields on the Email Message object with case-insensitive deterministic encryption, apply the scheme before you enter data into these fields. If existing data in these fields exceeds the following limits, that data isn't encrypted with case-insensitive deterministic encryption.

- API length: 527
- Byte length: 765
- Non-ASCII characters: 262

Case Comment Object

The Body field on the Case Comment object has a limit of 4,000 ASCII characters (or 4,000 bytes). However, when these fields are encrypted, the character limit is lower. How much lower depends on the kind of characters you enter.

- ASCII: 2959
- Chinese, Japanese, Korean: 1333
- Other non-ASCII: 1479

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

Which Salesforce Apps Don't Support Shield Platform Encryption?

Some Salesforce features work as expected when you work with data that's encrypted with Shield Platform Encryption. Others don't.

These apps don't support data encrypted with Shield Platform Encryption.

- Connect Offline
- Commerce Cloud (Salesforce B2B Commerce version 4.10 and later is supported)
- Data.com
- Einstein Recommendation Engine in Marketing Cloud (includes Einstein Recommendations, Einstein Web Recommendations, and Einstein Email Recommendations)
- Salesforce Einstein (includes Einstein Search, Sales Cloud Einstein, Einstein Discovery, Einstein Builders, and Einstein Vision and Language)
- Heroku (but Heroku Connect does support encrypted data)
- Marketing Cloud (but Marketing Cloud Connect does support encrypted data)
- Sales productivity features that require data to be stored using a public cloud provider
- Social Customer Service
- Thunder
- Quip
- Salesforce Billing

Legacy portals (customer, self-service, and partner) don't support data encrypted with Shield Platform Encryption. If legacy portals are active, Shield Platform Encryption can't be enabled.

 **Note:** This page is about Shield Platform Encryption, not Classic Encryption. [What's the difference?](#)

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Limit Interactions with External URLs and Origins

In our connected world, interaction with external websites and origins is a necessity. To protect your network and data, configure allowlists and enable settings that limit how Salesforce and external origins interact. And limit redirections that originate in Salesforce to URLs that you trust.

[Manage Trusted URLs](#)

Specify the URLs that you trust to interact with your users and network. Use Content Security Policy (CSP) directives to control the types of resources that Lightning components, third-party APIs, and WebSocket connections can load from each trusted URL. If you enabled the Permissions-Policy HTTP header in Session Settings, you can also control which URLs can access browser features from Salesforce.

[Review and Resolve CSP Violations](#)

To help prevent cross-site scripting (XSS) and other code injection attacks, Salesforce plans to update the system-defined trusted URLs in Summer '24. This change updates your content security policy (CSP), which controls which resources Lightning components, third-party APIs, and WebSocket connections can load. Use the CSP Violations list to identify the resources that are blocked with that change. Then, to allow the required resources, update your trusted URLs.

[Trust Redirections to Your Other Salesforce Orgs](#)

To protect your users from potential attacks, users can't access a different Salesforce org, including its publicly served pages and content, from your Salesforce org unless the URL is trusted. To allow a link, action, or process to take the user to a different Salesforce org that you own, add the target URL to the Trusted URLs for Redirects allowlist.

[Manage Redirections to External URLs](#)

Protect your users from untrusted external redirections from Salesforce Classic pages and components. First allowlist the external URLs that you trust. Specify what happens when a user clicks a link that takes them outside your Salesforce org. You can choose whether to alert users about untrusted external redirections or to block those redirections entirely.

[Configure Salesforce CORS Allowlist](#)

Cross-Origin Resource Sharing (CORS) allows web browsers to request resources from other origins. For example, using CORS, the JavaScript for a web application at `https://www.example.com` can request a resource from `https://www.salesforce.com`. To allow access to supported Salesforce APIs, Apex REST resources, and Lightning Out from JavaScript code in a web browser, add the requesting origin to your Salesforce CORS allowlist. For Lightning apps that allow web browsers to make requests from their orgs, CORS allowlist prevents requests to Lightning apps unless the request comes from an approved URL.

[Protect Sensitive Information in Your URLs](#)

To protect sensitive information in your URLs, such as an org ID, enable the referrer-policy HTTP header. When an action in Salesforce makes a request to another URL, the website receiving that request can see information about the origin. For example, when a Salesforce page loads an image, the website where the image lives can see the URL of that Salesforce page. And when you click a link, the website that you visit can see the URL of the Salesforce page where the link lives. The referrer-policy HTTP header controls how much of that URL, or referrer, is shared during that request.

[Protect Your Visualforce Pages with Cross-Origin Opener Policy \(COOP\)](#)

Help shield your custom Visualforce pages from external attacks. When you enable Cross-Origin Opener Policy (COOP), each top-level custom Visualforce page opens in a new browsing context group. This process prevents direct access between other browser tabs and your Visualforce page and the page's content.

[Restrict Page Resource Requests with Cross-Origin Embedder Policy \(COEP\)](#)

To safeguard your custom Visualforce pages, only allow content from external sources that trust your page. When you enable the Cross-Origin Embedder Policy (COEP) setting, externally sourced embedded content loads only when the origin explicitly states that your page or domain can load its content. Embedded content can include images, documents, and widgets.

Manage Trusted URLs

Specify the URLs that you trust to interact with your users and network. Use Content Security Policy (CSP) directives to control the types of resources that Lightning components, third-party APIs, and WebSocket connections can load from each trusted URL. If you enabled the Permissions-Policy HTTP header in Session Settings, you can also control which URLs can access browser features from Salesforce.

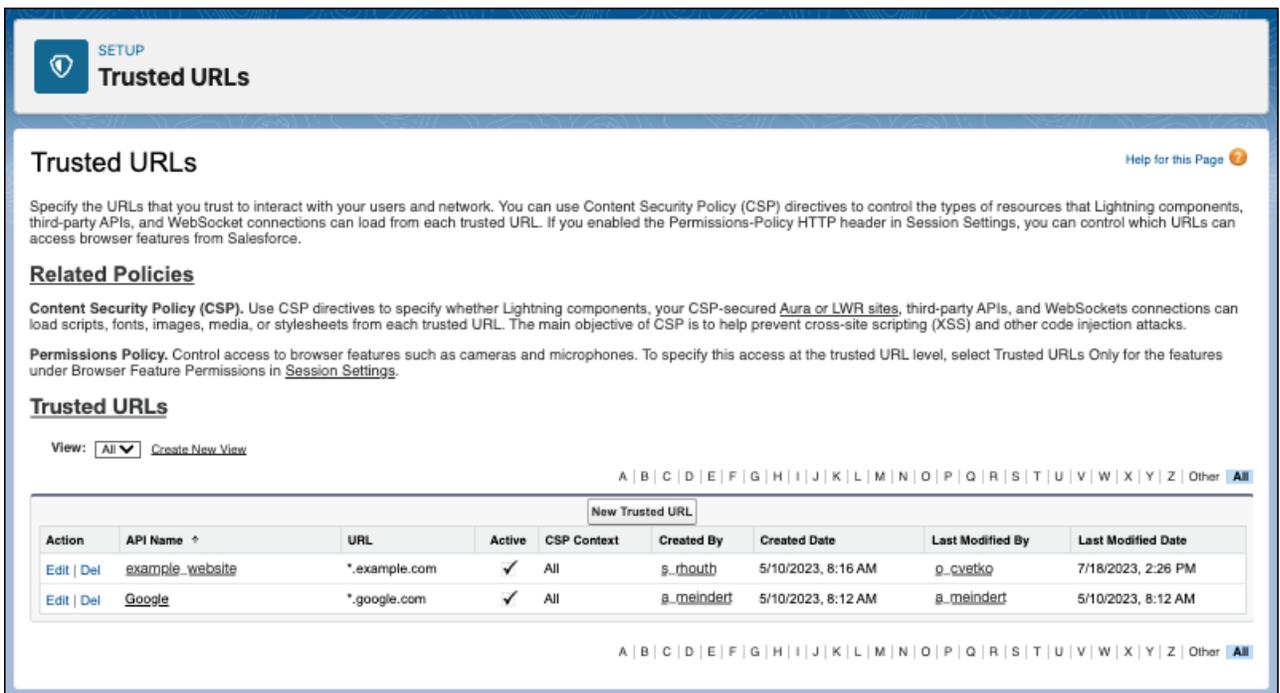
For each trusted URL in Setup, you can specify CSP directives and Permissions-Policy directives. To specify the external URLs to which users can be redirected from Salesforce, see [Manage Redirections to External URLs](#). To allow external sites to load your Visualforce pages or surveys in an inline frame (iframe), see [Specify Trusted Domains for Inline Frames](#).

 **Note:** To support integration across Salesforce products, Salesforce includes URLs in each CSP directive, even though those URLs aren't defined as trusted URLs. Salesforce regularly updates those URLs based on the latest requirements.

Add or Edit a Trusted URL

For each trusted URL in Setup, you can specify Content Security Policy (CSP) directives and Permissions-Policy directives.

1. From Setup, in the Quick Find box, enter *Trusted URLs*, and then select **Trusted URLs**.



Trusted URLs

Specify the URLs that you trust to interact with your users and network. You can use Content Security Policy (CSP) directives to control the types of resources that Lightning components, third-party APIs, and WebSocket connections can load from each trusted URL. If you enabled the Permissions-Policy HTTP header in Session Settings, you can control which URLs can access browser features from Salesforce.

Related Policies

Content Security Policy (CSP). Use CSP directives to specify whether Lightning components, your CSP-secured [Aura or LWR sites](#), third-party APIs, and WebSockets connections can load scripts, fonts, images, media, or stylesheets from each trusted URL. The main objective of CSP is to help prevent cross-site scripting (XSS) and other code injection attacks.

Permissions Policy. Control access to browser features such as cameras and microphones. To specify this access at the trusted URL level, select Trusted URLs Only for the features under Browser Feature Permissions in [Session Settings](#).

Trusted URLs

View: [Create New View](#)

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | Other **All**

Action	API Name	URL	Active	CSP Context	Created By	Created Date	Last Modified By	Last Modified Date
Edit Del	example_website	*.example.com	✓	All	s_rhouth	5/10/2023, 8:16 AM	p_cvetko	7/18/2023, 2:26 PM
Edit Del	Google	*.google.com	✓	All	g_meindert	5/10/2023, 8:12 AM	g_meindert	5/10/2023, 8:12 AM

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | Other **All**

2. To add a new trusted URL, click **New Trusted URL**.
3. To edit an existing trusted URL, click **Edit**.
4. If you're adding a trusted URL, enter the API Name.

Enter only underscores and alphanumeric characters. The name must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Performance, Developer, and Unlimited** Editions

USER PERMISSIONS

To create, read, update, and delete trusted URLs:

- Customize Application AND Modify All Data

If you edit the API name of an existing trusted URL, review your code and update references to the previous API name.

5. Edit or enter the URL.

The trusted URL must include a domain name and can include a port. For example, `https://example.com` or `https://example.com:8080`.

To reduce repetition, you can use the wildcard character * (asterisk). For example, `*.example.com`.

For a third-party API, the URL must begin with `https://`. For example, `https://example.com`.

For a WebSocket connection, the URL must begin with `wss://`. For example, `wss://example.com`.

6. Optionally, enter or edit a description for the trusted URL.

7. Optionally, to temporarily disable this trusted URL, deselect **Active**.

8. Specify at least one CSP directive or permissions policy directive for the trusted URL, and then save your changes.

Specify CSP Directives for a Trusted URL

To help prevent cross-site scripting (XSS) and other code injection attacks, the Lightning component framework uses Content Security Policy (CSP) to impose restrictions on content. By default, the framework's headers allow content to be loaded only from secure (HTTPS) URLs and forbid XHR requests from JavaScript. To use third-party APIs that make requests to an external (non-Salesforce) server or to use a WebSocket connection, add the server as a Trusted URL.

To enable the corresponding access for Apex, create a remote site.

 **Note:** Not every browser enforces CSP. For a list of browsers that enforce CSP, see caniuse.com

1. From Setup, in the Quick Find box, enter *Trusted URLs*, and then select **Trusted URLs**.

You define the CSP context and directives in the Content Security Policy (CSP) Settings section of the Trusted URL page.

Content Security Policy (CSP) Settings

To help prevent cross-site scripting (XSS) and other code injection attacks, the Lightning component framework uses CSP to impose restrictions on content. To control which pages can load content from this trusted URL, select the CSP context.

CSP Context: All

CSP Directives

Select the directives that Lightning components, third-party APIs, and WebSocket connections can load from this trusted URL. Each CSP directive controls access to a resource type. Lightning components can load the resources within Lightning or within your CSP-secured [Aura](#) or [LWR sites](#).

To use the [Salesforce Console Integration Toolkit](#) from within this trusted URL, select the `connect-src` (scripts) directive. Then add the trusted URL in the Security settings of Experience Builder for your [Visualforce sites](#). When you select that directive, connections from Lightning to this trusted URL can use the Javascript methods in the toolkit. Otherwise, you can't load JavaScript resources from a third-party, even if it's a trusted URL. To use a JavaScript library from a third-party, add the third-party URL to a static resource, and then add the static resource to your component.

<code>connect-src</code> (scripts)	<input type="checkbox"/>
<code>font-src</code> (fonts)	<input type="checkbox"/>
<code>frame-src</code> (iframe content)	<input type="checkbox"/>
<code>img-src</code> (images)	<input checked="" type="checkbox"/>
<code>media-src</code> (audio and video)	<input type="checkbox"/>
<code>style-src</code> (stylesheets)	<input type="checkbox"/>

2. To control which pages can load content from this trusted URL, select the CSP context.

a. To apply the CSP directives to all supported context types, select **All**. This context is the default.

b. To apply the CSP directives to Experience Cloud sites only, select **Experience Builder Sites**.

c. To apply the CSP directives to Lightning Experience pages only, select **Lightning Experience pages**.

- d. To apply the CSP directives to your custom Visualforce pages only, select **Visualforce Pages**.

For custom Visualforce pages, content is restricted to CSP Trusted Sites only if the page's `cspHeader` attribute is set to `true`.

 **Tip:** To specify CSP directives for one URL with two of the three CSP contexts, create two trusted URL records with different API names.

3. Select the CSP directives for this trusted URL. Each CSP directive controls access to a resource type. Lightning components can load the resources within Lightning or within your CSP-secured [Aura](#) or [LWR](#) sites.

- a. To allow Lightning components, third-party APIs, and WebSocket connections to load URLs that use script interfaces from this trusted URL, select **connect-src (scripts)**.

 **Note:** To use the Salesforce Console Integration Toolkit from within a trusted URL, also add the trusted URL in the Security settings of Experience Builder for your [Visualforce sites](#). Otherwise, you can't load JavaScript resources from a third party, even if it's a trusted URL.

To use a JavaScript library from a third party, add the library to a [static resource](#), and then add the static resource to your component.

- b. To allow Lightning components, third-party APIs, and WebSocket connections to load fonts from this trusted URL, select **font-src (fonts)**.
- c. To allow Lightning components, third-party APIs, and WebSocket connections to load resources contained in `<iframe>` elements from this trusted URL, select **frame-src (iframe content)**.
- d. To allow Lightning components, third-party APIs, and WebSocket connections to load images from this trusted URL, select **img-src (images)**. This option is enabled by default.
- e. To allow Lightning components, third-party APIs, and WebSocket connections to load audio and video from this trusted URL, select **media-src (audio and video)**.
- f. To allow Lightning components, third-party APIs, and WebSocket connections to load style sheets from this trusted URL, select **style-src (stylesheets)**.

4. After you save your changes, validate the header size for your Aura sites.

For Aura sites in Experience Cloud, if the HTTP header size is greater than 8 KB, the directives are moved from the CSP header to the `<meta>` tag. To avoid errors from infrastructure limits, we recommend that the header size doesn't exceed 3 KB per CSP context.

SEE ALSO:

[Configure Remote Site Settings](#)

[Secure Coding Guide: Secure Coding WebSockets](#)

[Lightning Aura Components Developer Guide: Content Security Policy Overview](#)

Grant a Trusted URL Access to Browser Features

Select the permissions policy directives for a trusted URL. Each directive grants the trusted URL access to a browser feature.

To use this feature, enable the Permissions-Policy header in Session Settings. You can control access to a browser feature at the trusted URL level only when access for the corresponding feature is set to Trusted URLs Only in Session Settings.

1. Add or edit a trusted URL.

You grant access to browser features in the Permissions Policy Directives section of the Trusted URL page.

Permissions Policy Directives

The pages that Salesforce delivers for this org include the Permissions-Policy HTTP header. Select the permissions policy directives for this trusted URL. Each directive grants the trusted URL access to a browser feature. For example, if the camera directive is enabled, scripts from this trusted URL can access the user's camera.

You can enable a directive only if access for the corresponding browser feature is set to Trusted URLs Only under Browser Feature Permissions in [Session Settings](#).

camera

microphone

2. To grant this trusted URL permission access to the user's camera, select **camera**.
3. To grant this trusted URL permission access to the user's camera, select **microphone**.

SEE ALSO:

[Limit Interactions with External URLs and Origins](#)

[Control Access to Browser Features](#)

Review and Resolve CSP Violations

To help prevent cross-site scripting (XSS) and other code injection attacks, Salesforce plans to update the system-defined trusted URLs in Summer '24. This change updates your content security policy (CSP), which controls which resources Lightning components, third-party APIs, and WebSocket connections can load. Use the CSP Violations list to identify the resources that are blocked with that change. Then, to allow the required resources, update your trusted URLs.

1. From Setup, in the Quick Find box, enter *CSP Violations*, and then select **CSP Violations**.
The CSP Violations list includes an entry for each unique combination of an external URL and CSP context with at least one CSP directive that's blocked with the upcoming change.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise, Performance, Developer,** and **Unlimited** Editions

USER PERMISSIONS

To view, filter, and delete CSP violations:

- Customize Application AND Modify All Data

To create, read, update, and delete trusted URLs:

- Customize Application AND Modify All Data

URL ↑	Context	Images	Fonts	IFrames	Last Violation Date
https://content.example.com	Lightning	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	12/1/2023, 1:32 PM
https://example.com	Communities	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	12/1/2023, 1:31 PM
https://img.example.com	Communities	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	12/1/2023, 1:31 PM
https://photos.example.com	Communities	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	12/1/2023, 1:31 PM
https://photos.example.com	Lightning	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	12/1/2023, 1:31 PM
https://play.vidyard.com	Lightning	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	12/5/2023, 10:08 AM

 **Note:** The CSP Violations list reflects the violations that are blocked in Summer '24. Until that release, these resources can be loaded in Salesforce.

- **URL**—The URL associated with the request, without the path. For example, if a blocked requested resource is an image with the URL `https://www.example.com/images/image1.png`, the URL on the CSP Violations list is `https://www.example.com`.
- **Context**—The CSP context for the request. The context controls which pages can load content from this trusted URL. Possible values are:
 - **Communities**—The blocked request is related to an Experience Builder site.
 - **Lightning**—The blocked request is related to a Lightning Experience page.
- **Image**—Indicates that at least one request to load an image file from the URL was blocked.
- **Font**—Indicates that at least one request to load a font from the URL was blocked.
- **iFrame**—Indicates that at least one request to load content in an iFrame that originated from the URL was blocked.
- **Latest Violation Date**—The latest recorded date of a violation for this URL, CSP context, and CSP directive.

If a resource request for a combination occurs more than one time, Salesforce updates the Latest Violation Date timestamp every 72 hours. For example, a request on a Lightning page for multiple images from a single URL occurs three times: February 21, 2024 at 8:11 AM, February 22, 2023 at 1:12 PM, and February 22, 2024 at 2:38 PM. The Latest Violation Date for the corresponding URL, context, and directive reflects the event on February 21, 2024 at 8:11 AM until Salesforce refreshes the data for this URL. Then the Latest Violation Date reflects the event on February 22, 2024 at 2:38 PM.

- To allow a CSP directive for a URL, note the URL, context, and directive. Then, on the CSP Violations list, click **Manage Trusted URLs**. On the Trusted URLs Setup page, check for an existing entry for the URL and context. Then either edit the existing trusted URL or add a new trusted URL and select the CSP directives to allow. For more information, see [Manage Trusted URLs](#).
- Optionally, remove items from the CSP Violations list.
 - To remove an item from the CSP Violations list, click  and select **Delete**.
 - To clear the logged violations for all URLs, click **Clear Violations Log** and confirm your decision.

When you remove an item from the CSP Violations list, no change is made to your trusted URLs and their CSP directives. Only the logged event is removed. If the CSP settings on your trusted URLs still block those requests, a new entry appears on the CSP Violations list the next time a matching request occurs.

SEE ALSO:

[Limit Interactions with External URLs and Origins](#)

[Manage Trusted URLs](#)

Trust Redirections to Your Other Salesforce Orgs

To protect your users from potential attacks, users can't access a different Salesforce org, including its publicly served pages and content, from your Salesforce org unless the URL is trusted. To allow a link, action, or process to take the user to a different Salesforce org that you own, add the target URL to the Trusted URLs for Redirects allowlist.

 **Note:** This topic applies to redirections to other Salesforce orgs. For example, when a user clicks a link in a sandbox that brings them to production. For settings related to other links that take users outside your Salesforce org, see [Manage Redirections to External URLs](#).

There are two primary methods to redirect a user to another org: a direct link, or a parameter within the code. An example of a direct link is a hyperlink on a Visualforce page. An example of a parameter that redirects the user is `saveURL`, which defines where to redirect the user when they click the Save button.

When you prevent untrusted cross-org redirections, Salesforce verifies the initial redirection outside of Salesforce against the Trusted URLs for Redirects allowlist. Subsequent redirections can't be verified because they occur outside Salesforce.

Cross-org redirections are a specific kind of cross-origin redirection. Salesforce allows cross-origin redirections within the same org. For example, a redirection from `MyDomainName.my.salesforce.com` to `MyDomainName.my.file.force.com`. Also, when you change your My Domain and redirections from your previous My Domain are enabled, cross-origin redirections from your previous My Domain URLs are allowed. For example, a redirection from `OldMyDomainName.my.salesforce.com` to `NewMyDomainName.lightning.force.com` is allowed, because those URLs belong to the same org. A cross-org redirection takes the user from one Salesforce org to another. For example, from `MyDomainName--UAT.sandbox.lightning.force.com` to `MyDomainName.my.salesforce.com`.

To search your Salesforce code or cross-org redirections, download the metadata for each of your Salesforce orgs via a tool such as [Salesforce CLI](#). Then use a code editor such as Microsoft Visual Studio to search for URLs that belong to your other Salesforce orgs. For a list of the hostname formats for Salesforce orgs, see [My Domain URL Formats](#).

 **Tip:** Also add your custom domains to the Trusted URLs for Redirects allowlist. A custom domain is a domain that you own, such as `https://www.example.com`, that serves content from your Experience Cloud sites or Salesforce Sites. You can find your custom domains on the Domains page in Setup.

1. To avoid unnecessary redirections, update incorrect links.

If you use hard-coded links, that link can be copied from production to a sandbox, resulting in an incorrect URL. For example, on a Visualforce page in a sandbox, you find a link to a file that lives in production. To link to the file in the sandbox instead, update the link to use the corresponding sandbox URL. Use relative or dynamically generated URLs whenever possible.
2. If the redirection is valid, add the target URL to the Trusted URLs for Redirects allowlist. For example, if you own multiple production orgs and use redirections to route the user to the correct org, trust the URLs for the other production orgs.
 - a. From Setup, in the Quick Find box, enter *Trusted URLs for Redirects*, and then select **Trusted URLs for Redirects**.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

USER PERMISSIONS

To set up trusted URLs for redirects:

- [Customize Application AND Modify All Data](#)

- b. Click **New URL**.
- c. Enter the URL, and save your changes.

These formats are accepted: `example.com`, `*.example.com`, and `https://example.com`.

If you use a wildcard to allow redirections to your other Salesforce orgs, ensure that the value after the wildcard is unique to the org that you trust. Usually this approach requires that the trusted URL includes the My Domain name of the trusted org. For example, to trust `https://MyDomainName.file.force.com`, trust the full URL or `*.MyDomainName.file.force.com`.



Warning: To protect your users, we highly discourage adding top-level Salesforce domains, such as `*.salesforce.com`, `*.force.com`, or in this case, `*.file.force.com`, to the Trusted URLs for Redirects allowlist.

3. To restrict cross-org redirections to the Salesforce org URLs on your allowlist, disable **Allow untrusted cross-org redirections** on the Trusted URLs for Redirects Setup page.



Note: This setting is available in Lightning Experience only. If you can't access the Trusted URLs for Redirects Setup page in Lightning Experience, use the `enableCrossOrgRedirects` field in the [SessionSettings](#) metadata API type.

When this setting is enabled, no warning is displayed to the user when they're redirected to another Salesforce org.

SEE ALSO:

[Limit Interactions with External URLs and Origins](#)

Manage Redirections to External URLs

Protect your users from untrusted external redirections from Salesforce Classic pages and components. First allowlist the external URLs that you trust. Specify what happens when a user clicks a link that takes them outside your Salesforce org. You can choose whether to alert users about untrusted external redirections or to block those redirections entirely.

This topic applies to links in components and pages built in Salesforce Classic that take users to a non-Salesforce domain. To allow redirections to other Salesforce orgs in both Salesforce Classic and Lightning Experience, see [Trust Redirections to Your Other Salesforce Orgs](#).

Salesforce verifies the initial redirection outside of Salesforce against the Trusted URLs for Redirects allowlist. However, Salesforce can't verify subsequent redirections. For example, if a link on a Visualforce page takes the user to `https://www.example.com`, Salesforce verifies that you allowed redirections to `https://www.example.com`. If that URL then redirects the user to `https://spam.example.com`, Salesforce can't check that redirection, because it occurs outside of Salesforce.



Note: Except for cross-org redirections, you can't restrict redirections that originate from pages and components built with Lightning Experience.

Allow the URLs that You Trust for External Redirections from Salesforce Classic Pages and Components

Help your users navigate to the URLs that you trust from pages and components built in Salesforce Classic. Add your trusted URLs to the Trusted URLs for Redirects allowlist. Connections from Salesforce to URLs in that allowlist are always allowed without a warning.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in: all editions

USER PERMISSIONS

To modify session security settings:

- Customize Application

To set up trusted URLs for redirects:

- Customize Application AND Modify All Data

 **Tip:** Include your custom domains in the Trusted URLs for Redirects allowlist. A custom domain is a domain that you own, such as `https://www.example.com`, that serves content from your Experience Cloud sites or Salesforce Sites. You can find your custom domains on the Domains page in Setup.

1. From Setup, in the Quick Find box, enter *Trusted URLs for Redirects*, and then select **Trusted URLs for Redirects**.
2. Click **New URL**.
3. Enter the URL, and save your changes.
These formats are accepted: `example.com`, `*.example.com`, and `https://example.com`.

Secure External Redirections from Salesforce Classic Pages and Components

Finish protecting your users during redirections from pages and components built in Salesforce Classic. Either block external redirections to URLs that aren't on the Trusted URLs for Redirects allowlist or warn users during those redirections.

1. From Setup, in the Quick Find box, enter *Session Settings*, and then select **Session Settings**.
2. Under External Redirections, in the Allow redirections to untrusted external URLs field, specify the desired behavior when a user clicks an untrusted external link from a page or component built in Salesforce Classic.
 - To block redirections to untrusted external URLs, select **Never**. A message informs the user that they can't access the page because the external site isn't trusted.
 - To show a warning message that requires the user to confirm that they want to leave the current page before they're redirected, select **With user's permission**.

The Always option isn't recommended because it allows redirections to untrusted external URLs without a warning.

3. Save your changes.

SEE ALSO:

[Limit Interactions with External URLs and Origins](#)

Configure Salesforce CORS Allowlist

Cross-Origin Resource Sharing (CORS) allows web browsers to request resources from other origins. For example, using CORS, the JavaScript for a web application at `https://www.example.com` can request a resource from `https://www.salesforce.com`. To allow access to supported Salesforce APIs, Apex REST resources, and Lightning Out from JavaScript code in a web browser, add the requesting origin to your Salesforce CORS allowlist. For Lightning apps that allow web browsers to make requests from their orgs, CORS allowlist prevents requests to Lightning apps unless the request comes from an approved URL.

These Salesforce technologies support CORS.

- Apex REST
- Bulk API
- Bulk API 2.0
- Connect REST API
- Lightning Out
- REST API
- CRM Analytics REST API
- User Interface API

Add an origin serving the request code to the CORS allowlist. If a browser that supports CORS makes a request to an origin in the allowlist, Salesforce returns the origin in the

`Access-Control-Allow-Origin` HTTP header along with any additional CORS HTTP headers. If the origin isn't included in the allowlist, Salesforce returns HTTP status code 403.

1. From Setup, in the Quick Find box, enter `CORS`, and then select **CORS**.
2. Select **New**.
3. Enter a resource in Origin URL Pattern.



Tip: The origin URL pattern doesn't always match the URL that appears in your browser's address bar.

4. Save your changes.

The origin URL pattern must include the HTTPS protocol (unless you're using your localhost) and a domain name. It can also include a port. The wildcard character (*) is supported and must be in front of a second-level domain name. For example, `https://*.example.com` adds all subdomains of `example.com` to the allowlist.

The origin URL pattern can be an IP address. But an IP address and a domain that resolve to the same address aren't the same origin, and you must add them to the CORS allowlist as separate entries.

Google Chrome™ and Mozilla® Firefox® browser extensions are allowed as resources in API version 53 (Winter '22) or later. Chrome extensions must use the prefix `chrome-extension://` and 32 characters without digits or capital letters, for example `chrome-extension://abdckegmcbiomijcbdaodaf1gehffed`. Firefox extensions must use the prefix `moz-extension://` and an 8-4-4-4-12 format of small alphanumeric characters, for example `moz-extension://1234ab56-78c9-1df2-3efg-4567891hi1j2`.

You can get a successful response when requesting a REST resource in a CORS preflight test, but receive an unsuccessful response to the actual request. This discrepancy can occur when the resource is deleted after the preflight test and before the request is made. It can also occur if the resource doesn't exist. A CORS preflight confirms if resources can be passed between servers, but doesn't check if a specific resource exists or not. CORS preflight requests are typically issued automatically by a browser.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Developer, Enterprise, Performance, and Unlimited** Editions

Available with API access enabled in: Professional Edition

USER PERMISSIONS

To create, read, update, and delete:

- **Modify All Data**

 **Note:** To access certain OAuth endpoints with CORS, other requirements apply. See https://help.salesforce.com/s/articleView?id=sf.remoteaccess_oauth_endpoints_cors.htm.

SEE ALSO:

[Limit Interactions with External URLs and Origins](#)

Protect Sensitive Information in Your URLs

To protect sensitive information in your URLs, such as an org ID, enable the referrer-policy HTTP header. When an action in Salesforce makes a request to another URL, the website receiving that request can see information about the origin. For example, when a Salesforce page loads an image, the website where the image lives can see the URL of that Salesforce page. And when you click a link, the website that you visit can see the URL of the Salesforce page where the link lives. The referrer-policy HTTP header controls how much of that URL, or referrer, is shared during that request.

1. From Setup, in the Quick Find box, enter *Session Settings*, and then select **Session Settings**.
2. In the Referrer URL Protection section, select **Include Referrer-Policy HTTP header**.
When this setting is enabled, all pages served by Salesforce include the `referrer-policy` HTTP header. When this setting is disabled, browsers use their default referrer-policy directive, which usually exposes your full URL.
3. Select an HTTP Referrer Policy.
 - a. To send the origin only for cross-domain requests and when the target website is on a downgraded protocol, select **origin-when-cross-origin**.
This setting is the default setting.
 - b. To never include the referrer, select **no-referrer**.
 - c. To omit the referrer when the target website is on a downgraded protocol, select **no-referrer-when-downgrade**.
This option isn't recommended because the full URL of the page is exposed to cross-origin requests to the same or a higher protocol level. For example, requests from HTTPS to HTTPS and requests from HTTP to either HTTP or HTTPS.
 - d. To always send the origin only, select **origin**.
 - e. To omit the referrer for cross-origin requests, select **same-origin**.
 - f. To send the origin only for requests with the same protocol level and to omit the referrer when the target website is on a downgraded protocol, select **strict-origin**.
 - g. To send the referrer URL for same-origin requests, to send the origin only for cross-origin requests on the same protocol, and to omit the referrer when the target website is on a downgraded protocol, select **strict-origin-when-cross-origin**.
 - h. To always include the referrer URL, select **unsafe-url**.
This option isn't recommended because the full URL of the page is exposed to requests from insecure origins.
4. Save your changes.

 **Example:** Let's look at how URLs are shared with the strict-origin-when-cross-origin HTTP Referrer Policy.

Start on your user profile on an Experience Cloud site with the URL

`https://MyDomainName.my.site.com/pageName/s/profile/userId`. When you click a link on your profile

EDITIONS

Available in: Lightning Experience and Salesforce Classic (not available in all orgs)

Available in: **Essentials, Personal, Contact Manager, Group, Professional, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

USER PERMISSIONS

To modify session security settings:

- Customize Application

to another Experience Cloud site page with the URL `https://MyDomainName.my.site.com/pageName`, both URLs are on the `site.com` domain, and both URLs use the HTTPS protocol. So the full URL of your user profile is shared as the referrer.

That Experience Cloud site page includes an embedded image with the URL

`http://example.com/images/header_image.png`. Loading that image is an example of a request with a downgraded protocol because the site page uses HTTPS but the target URL uses HTTP. The request to load the image includes no referrer information.

Then you click a link on that Experience Cloud site page to access a report with the URL

`https://MyDomainName.lightning.force.com/lightning/r/Report/reportId/view`. This action initiates a cross-origin request because `site.com` and `force.com` are different domains. And both URLs use the same protocol: HTTPS.

So in this case, the request includes only the origin as the referrer. The origin is the URL without the path, in this case,

`https://MyDomainName.my.site.com`. A request to an external website on the same protocol, such as

`https://www.example.com`, also includes only the origin as the referrer.

For more information on HTTP Referrer Policy values, including examples, see the [Referrer-Policy](#) entry in the *MDN Docs HTTP Guide*.

SEE ALSO:

[Limit Interactions with External URLs and Origins](#)

Protect Your Visualforce Pages with Cross-Origin Opener Policy (COOP)

Help shield your custom Visualforce pages from external attacks. When you enable Cross-Origin Opener Policy (COOP), each top-level custom Visualforce page opens in a new browsing context group. This process prevents direct access between other browser tabs and your Visualforce page and the page's content.

COOP helps to shield your Visualforce pages from cross-site scripting (XSS), a type of security vulnerability. With XSS, an attacker includes malicious code in a client-side script in a legitimate web page or web application. When a user visits the page or application, the web page or application delivers the malicious script to the user's browser.

With COOP, each top-level custom Visualforce page opens in a new browsing context group. Browser content that your Visualforce page opens within an iframe can access the parent page. However, processes that attempt to open your page in a new tab or pop-up window can't access the page for potential cross-origin attacks.

 **Note:** To preserve your users' access to required content, we recommend that you review the expected behavior and test COOP in a sandbox before you enable this feature in production.

Browser access checks use the headers for both your Visualforce page and the external sites that you access from your page. The combination of Cross-Origin Opener Policy (COOP) and Cross-Origin Embedder Policy (COEP) headers determines whether the Visualforce page and external sites can interact. To learn more about COOP and COEP, we recommend these topics on MDN Web Docs: [Cross-Origin-Opener-Policy](#) and [Cross-Origin-Embedder-Policy](#).

1. From Setup, in the Quick Find box, enter `Session Settings`, and then click **Session Settings**.
2. In the Visualforce Cross-Origin Security Headers section, select **Cross-Origin Opener Policy (COOP)**.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To modify session security settings:

- Customize Application

3. Save your changes.

SEE ALSO:

[Limit Interactions with External URLs and Origins](#)

[Restrict Page Resource Requests with Cross-Origin Embedder Policy \(COEP\)](#)

Restrict Page Resource Requests with Cross-Origin Embedder Policy (COEP)

To safeguard your custom Visualforce pages, only allow content from external sources that trust your page. When you enable the Cross-Origin Embedder Policy (COEP) setting, externally sourced embedded content loads only when the origin explicitly states that your page or domain can load its content. Embedded content can include images, documents, and widgets.

When COEP is enabled, externally sourced embedded content loads only when the external origin allows it via one of these methods.

 **Note:** To preserve your users' access to required content, we recommend that you review the expected behavior and test COEP in a sandbox before you enable this feature in production.

Browser access checks use the headers for both your Visualforce page and the external sites that you access from your page. The combination of Cross-Origin Embedder Policy (COEP) and Cross-Origin Opener Policy (COOP) headers determines whether the Visualforce page and external sites can interact. To learn more about COOP and COEP, we recommend these topics on MDN Web Docs: [Cross-Origin-Opener-Policy](#) and [Cross-Origin-Embedder-Policy](#).

- Cross Origin Resource Policy (CORP). The externally sourced content includes the Cross-Origin-Resource-Policy header with the cross-origin value.
 - Cross-Origin Resource Sharing (CORS). The external origin includes your page or its domain in its CORS allowlist. When your page makes a request, the external origin responds with the required Access-Control-Allow-* headers that allow your page access to the content.
1. From Setup, in the Quick Find box, enter *Session Settings*, and then click **Session Settings**.
 2. In the Visualforce Cross-Origin Security Headers section, select **Cross-Origin Embedder Policy (COEP)**.

 **Note:** COEP applies to all your custom Visualforce pages.

3. Save your changes.

SEE ALSO:

[Limit Interactions with External URLs and Origins](#)

[Protect Your Visualforce Pages with Cross-Origin Opener Policy \(COOP\)](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To modify session security settings:

- Customize Application

Configure Clickjack Protection

Clickjacking is a type of attack that tricks users into clicking something, such as a button or link. The click sends an HTTP request that performs malicious actions that can lead to data intrusion, unauthorized emails, changed credentials, or similar results. To help protect against this kind of attack, most Salesforce pages can only be served in an inline frame by a page on the same domain. Learn which types of pages can be framed and how to configure the related clickjack settings.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Clickjack Protection

Clickjacking uses a trusted domain or site to trick users into clicking a malicious link. With clickjacking, the trusted domain is served in an iframe, then a hidden or transparent UI control is served in the same location. For example, a transparent button on top of the Save button. The user thinks that they're clicking the top-level iframe when they're really clicking the hidden UI control.

To protect your users, Salesforce uses clickjack protection. For pages that Salesforce serves, clickjack protection is implemented through the Content Security Policy (CSP) `frame-ancestors` HTTP response header directive. An HTTP response header is part of the HTTP response passed from a server to a browser or client machine in response to an HTTP request. Within that header, a directive is a value that provides additional context or instructions. The CSP `frame-ancestors` HTTP response header directive tells the browser which sites are allowed to load the page in an iframe.

Salesforce applies the CSP `frame-ancestors` HTTP response header directive to the pages that Salesforce serves when that directive is supported. To expand clickjack protection to more users, you can include that directive in the rare cases when Salesforce can't identify whether the requesting app or specialized browser supports the directive. For more information, see [Apply Clickjack Protection to Less Common Browsers](#).

Three CSP `frame-ancestors` values apply in Salesforce. The page type determines whether that HTTP response header is present by default and which of these options are available within the header.

- `'none'`—prevents loading this page in an iframe.
- `'self'`—pages from the same origin as the protected page, including the same URL scheme and port number, can load this page in an iframe.
- A list of domains—the domains that can load this page in an iframe. The list can include wildcards. For example, `*.force.com`. Usually, this option is combined with the `'self'` value.

 **Note:** The CSP `frame-ancestors` header directive replaces the obsolete `X-Frame-Options` header. For more information, see [X-Frame-Options](#) on the *Mozilla Developer Network*.

Salesforce Login Pages

External sites can't frame Salesforce login pages, including generic login pages, such as `https://login.salesforce.com`. Also, external sites can't frame your org's My Domain login page, such as `https://mycompany.my.salesforce.com`. For these pages, the CSP `frame-ancestors` HTTP response header is set to `'none'`, and you can't change the HTTP response header.

Lightning Pages

Lightning pages delivered by Salesforce as part of the Platform can frame Lightning pages within the same org. The URLs for these pages contain `lightning.force.com` and a unique identifier in the form of a 16-digit number. For these pages, the CSP `frame-ancestors` HTTP response header is set to `'self'`, and you can't change the HTTP response header directive.

For details on clickjack protection options for your Experience Cloud site's Lightning page, see the section of this topic on Experience Cloud sites.

Salesforce Classic Pages

External sites can't frame pages built in Salesforce Classic and delivered by Salesforce. Examples of Salesforce Classic Pages include Setup pages and the pages for Salesforce objects, such as the Account detail page. Although users can view these pages in Lightning mode, the pages were built using Salesforce Classic.

Two Session Settings prohibit framing of Classic pages delivered by Salesforce: **Enable clickjack protection for Setup pages** and **Enable clickjack protection for non-Setup Salesforce pages**. These settings are enabled by default and can't be disabled. To disable these settings, contact Salesforce Customer Support.

Visualforce Pages

By default, Visualforce pages can be loaded in an iframe. For Visualforce pages with headers, the CSP `frame-ancestors` HTTP response header directive is absent.

To prevent external websites from loading your Visualforce pages in an iframe, enable two session settings. Then you can optionally define the external domains that you trust to frame your Visualforce pages. For more information, see [Enable Clickjack Protection for Visualforce Pages](#) and [Specify Trusted Domains for Inline Frames](#) in Salesforce Help.

Experience Cloud Sites

By default, Experience Cloud site pages can frame other site pages with the same domain and protocol security. The CSP `frame-ancestors` HTTP response header directive for these pages is set to `'self'`.

You can allow trusted external domains to frame your site pages through page-level settings. For Experience Builder site pages, clickjack settings are in the Security & Privacy settings. For Salesforce Tabs and Visualforce Sites, clickjack settings are in the page administration for Force.com sites in Experience Workspaces.

For more information, see [Enable Clickjack Protection in Experience Cloud Sites](#) in Salesforce Help.

Salesforce Sites and Force.com Sites

By default, a page within Salesforce Sites and Force.com Sites can frame other site pages with the same domain and protocol security. The CSP `frame-ancestors` HTTP response header directive for these pages is set to `'self'`.

You can allow trusted external domains to frame your site pages through page-level site configuration settings. To set the clickjack protection level and trusted domains for each page, edit the configuration in Site.com Studio. For more information, see [Enable Clickjack Protection in Site.com](#) in Salesforce Help.

Surveys

By default, Surveys can be framed by pages with the same domain and protocol security. The CSP `frame-ancestors` HTTP response header directive is set to `'self'`.

Optionally, you can define the external domains that you trust to frame the surveys for your org. For more information, see [Specify Trusted Domains for Inline Frames](#) in Salesforce Help.

SEE ALSO:

[Session Security](#)

[Mozilla Developer Network: CSP: frame-ancestors](#)

Enable Clickjack Protection for Visualforce Pages

To help protect against clickjack attacks, prevent external sites from loading your Visualforce pages in an inline frame (iframe). Optionally, you can allow trusted external sites to frame your Visualforce pages.

1. From Setup, in the Quick Find box, enter *Session Settings*, and then select **Session Settings**.

The two settings under Clickjack Protection for Visualforce pages refer to whether headers are enabled. The `apex:page` field `showHeader` indicates whether headers are enabled on a page.

2. To allow other Visualforce pages to frame Visualforce pages with headers enabled, select **Enable clickjack protection for customer Visualforce pages with standard headers**.
3. To allow other Visualforce pages to frame Visualforce pages with headers disabled, select **Enable clickjack protection for customer Visualforce pages with headers disabled**.
4. Save your changes.

When you save your session settings with at least one of the options enabled, the CSP `frame-ancestors` HTTP response header for the corresponding Visualforce pages is set to `'SELF'`. And any trusted domains for inline frames for Visualforce pages included in the same HTTPS response header.

To allow trusted external sites to load your Visualforce pages in an iframe, add each domain that you trust to the allowlist in Session Settings. For more information, see [Specify Trusted Domains for Inline Frames](#) in Salesforce Help.

SEE ALSO:

- [Configure Clickjack Protection](#)
- [Salesforce Feedback Management](#)
- [Apply Clickjack Protection to Less Common Browsers](#)

Specify Trusted Domains for Inline Frames

To allow external sites to load your Visualforce pages or surveys in an inline frame (iframe), add the domain to an allowlist in Session Settings.

-  **Note:** To specify trusted domains for Experience Cloud sites and Salesforce Sites, see [Enable Clickjack Protection for Experience Builder Sites](#) and [Enable Clickjack Protection in Site.com](#) in Salesforce Help.

1. From Setup, in the Quick Find box, enter *Session Settings*, and then select **Session Settings**.
2. In the Trusted Domains for Inline Frames section of the Session Settings Setup page, click **Add Domain**.

3. Enter the domain.

Acceptable formats are `example.com`, `https://example.com`, and `*.example.com`.

4. Select the allowed IFrame Type for this domain.
 - a. To allow the specified domain to load Visualforce pages in an iframe, select **Visualforce Pages** and save your changes.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To modify session security settings:

- Customize Application

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To modify session security settings:

- Customize Application

If clickjack protection is enabled for the Visualforce page, the domain is added to the Content Security Policy (CSP) `frame-ancestors` HTTP response header for the corresponding Visualforce pages. For example, `'self' abc.com *.my.site.com`. For more information, see [Enable Clickjack Protection for Visualforce Pages](#) in Salesforce Help.

If clickjack protection isn't enabled for the Visualforce page, then all external websites can load the Visualforce page in an iframe. For more information, see [Configure Clickjack Protection](#) in Salesforce Help.

- b.** To allow the specified domain to load surveys in an iframe, select **Surveys** and save your changes.

The domain is added to the CSP `frame-ancestors` HTTP response header for Survey pages. For example, `'self' abc.com *.my.site.com`.

5. To edit a domain in your Trusted Domains for Inline Frames list, click **Edit** for that domain.
6. To delete a domain in your Trusted Domains for Inline Frames list, click **Del** for that domain.

SEE ALSO:

[Configure Clickjack Protection](#)

[Apply Clickjack Protection to Less Common Browsers](#)

Apply Clickjack Protection to Less Common Browsers

To help protect your users against clickjacking attacks, Salesforce applies the Content-Security-Policy: `frame-ancestors` HTTP header directive to the pages that Salesforce serves when that directive is supported. To extend clickjack protection to more users, include that directive in the rare cases when Salesforce can't identify whether the requesting app or specialized browser supports the directive.

The supported browsers and devices for Salesforce Lightning Experience and Salesforce Classic support the required HTTP header directive for clickjacking protection. We recommend that you enable this feature only if your users access Salesforce via unsupported apps or specialized browsers with unclear support for Content-Security-Policy: `frame-ancestors`.

 **Warning:** When this option is enabled, users who access Salesforce via an app or browser that doesn't support the Content-Security-Policy: `frame-ancestors` directive can experience errors if that lack of support is unclear. We encourage you to test this feature in a sandbox via your users' apps and browsers. Then weigh the benefit of the additional clickjack protection against the errors that users can experience.

1. From Setup, in the Quick Find box, enter *Session Settings*, and then select **Session Settings**.
2. In the Content Security Policy (CSP) Directive Rendering section, select **Apply CSP directives for less common browsers**, and then save your changes.

SEE ALSO:

[Configure Clickjack Protection](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To modify session security settings:

- Customize Application

Session Security

After logging in, a user establishes a session with the platform. Use session security to limit exposure to your network when a user leaves the computer unattended while still logged in. Session security also limits the risk of internal attacks, such as when one employee tries to use another employee's session. Choose from several session settings to control session behavior.

You can control when an inactive user session expires. The default session timeout is two hours of inactivity. When the session timeout is reached, users are prompted with a dialog that allows them to log out or continue working. If they don't respond to this prompt, they're logged out.

 **Note:** When users close a browser window or tab, they aren't automatically logged out from their Salesforce session. Ensure that your users are aware of this behavior and that they end all sessions properly by selecting *Your Name* > **Logout**.

User sessions can expire when a new Salesforce major release takes effect. To avoid disruptions, start a new session after a major release. To see major release dates for your instance, go to [Trust Status](#), search for your instance, and click the maintenance tab.

You can restrict access to certain types of resources based on the security level associated with the authentication method for the user's current session. By default, each login method has one of two security levels: Standard or High Assurance. You can change the session security level and define policies so that specified resources are available only to users assigned a High Assurance level. For details, see [Session-level Security in Modify Session Security Settings](#) on page 1032.

You can control whether your org stores user logins and whether they can appear from the Switcher with the settings **Enable caching and autocomplete on login page**, **Enable user switching**, and **Remember me until logout**.

[Modify Session Security Settings](#)

Use the Session Settings screen to configure session security. You can configure settings such as the session connection type, timeout restrictions, and IP address ranges to protect against malicious attacks.

[Enable Browser Security Settings](#)

Browser security settings protect sensitive information and monitor SSL certificates.

[Set Trusted IP Ranges for Your Organization](#)

Trusted IP Ranges define a list of IP addresses from which users can log in without receiving a login challenge for verification of their identity, such as a code sent to their mobile phone.

[Control Access to Browser Features](#)

To control whether requests to an external (non-Salesforce) server or URL can access the user's camera and microphone, enable the Permissions-Policy HTTP header. Then select when to allow access to each of these browser features.

[Require High-Assurance Session Security for Sensitive Operations](#)

To secure different setup areas in your org, require a high-assurance level of security for sensitive operations, such as accessing reports and managing IP addresses. You can also block users from accessing these setup areas.

[View User Session Information on the Session Management Page](#)

Monitor and protect Salesforce by reviewing active sessions and session details on the Session Management page in Setup. You can create custom list views, view details about a user associated with a specific session, and easily end suspicious sessions. Salesforce admins can view all active user sessions, and non-admins see only their sessions.

[User Session Types](#)

Learn about the session types in the User Session Information page to help you monitor and protect your org.

[Salesforce Platform Cookies](#)

The Salesforce Platform uses cookies to improve functionality and accelerate processing times. By saving a user's settings, cookies can enhance the user's experience and the Salesforce Platform's performance.

[Using Frontdoor.jsp to Bridge an Existing Session Into Salesforce](#)

You can use frontdoor.jsp to give users access to Salesforce from a custom web interface, such as a Salesforce site, using their existing session ID and the server URL.

SEE ALSO:

[Set Trusted IP Ranges for Your Organization](#)

Modify Session Security Settings

Use the Session Settings screen to configure session security. You can configure settings such as the session connection type, timeout restrictions, and IP address ranges to protect against malicious attacks.

Configure these settings on the Session Settings page.

- [Configure Session Timeout Settings](#)
- [Configure Session Settings](#)
- [Configure Secure Connections \(HTTPS\) Settings](#)
- [Configure Caching Settings](#)
- [Cross-Site Request Forgery Protection](#)
- [Configure Content Security Policy Protection](#)
- [Configure Lightning Locker API Version Setting](#)
- [Configure Lightning Web Security](#)
- [Configure Extra Protection for Your Sessions](#)
- [Configure Session Security Levels](#)
- [Configure High Assurance Sessions for Reports, Dashboards, and Connected Apps](#)
- [Configure Logout Page Settings](#)
- [Configure Session Settings for New User Email](#)

 **Note:** Identity verification settings are also available on the Identity Verification page. You can change identity verification settings in either location. For information about configuring these settings, see [Define Identity Verification Settings for Your Orgs and Experience Cloud Sites](#).

SEE ALSO:

[Session Security](#)
[Define Identity Verification Settings for Your Orgs and Experience Cloud Sites](#)
[Require High-Assurance Session Security for Sensitive Operations](#)
[Network Best Practices](#)

Configure Session Timeout Settings

1. From Setup, in the Quick Find box, enter *Session Settings*, and then select **Session Settings**.
2. For **Timeout Value**, select the length of time after which the system logs out inactive users. For portal users, even though the actual timeout is between 10 minutes and 24 hours, you can only select a value between 15 minutes and 24 hours. If you want to enforce stricter security for sensitive information, choose a shorter timeout period.

EDITIONS

Available in:

EDITIONS

Available in: Lightning Experience and Salesforce Classic ([not available in all orgs](#))

The Lock sessions to the IP address from which they originated setting is available in: **Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

All other settings available in: **Essentials, Personal, Contact Manager, Group, Professional, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

USER PERMISSIONS

To modify session security settings:

- [Customize Application](#)

 **Note:** Salesforce updates the last active session time value every 5 minutes. So if you have a 30-minute timeout and you update a record at the 3-minute mark, Salesforce checks for activity and refreshes your session at the 5-minute mark. If you don't make any other updates, the total length of the session is 35 minutes.

3. To disable the timeout warning message for inactive users, select **Disable session timeout warning popup**. When this parameter isn't selected, a timeout warning message prompts inactive users 30 seconds before timeout, or as specified by the timeout value.
4. To invalidate timed-out sessions for inactive users, select **Force logout on session timeout**. The browser refreshes and returns to the login page, and the user must log in again for access.

 **Note:** When this setting is enabled, don't select **Disable session timeout warning popup**.

Configure Session Settings

1. From Setup, in the Quick Find box, enter *Session Settings*, then select **Session Settings**.
2. To lock the IP address from which the user logged in, select **Lock sessions to the IP address from which they originated**. Locking the IP address helps to prevent unauthorized persons from hijacking a valid session.

 **Note:** This setting can inhibit various applications and mobile devices.

3. Optionally, enable **Terminate all of a user's sessions when an admin resets that user's password**. This setting helps you mitigate security incidents such as stolen passwords and credential stuffing attacks. If you suspect that a user's password is compromised, you can reset that user's password and terminate all of their UI sessions at the same time. This setting also applies when you reset passwords for multiple users at once.
4. To associate a current UI session for a user with a specific domain, select **Lock sessions to the domain in which they were first used**. For example, associate an Experience Cloud site user with the site domain. This setting helps prevent unauthorized use of the session ID in another domain. This setting is enabled by default for Salesforce orgs created with the Spring '15 release or later.
5. Optionally, enable **Allow employees to log in directly to an Experience Cloud site** (recommended). With this setting, your internal users can use their internal username and password on the site login page. Employees must be members of the site to log in directly from the site login page. After they log in, your internal users land on the site home page.
6. Optionally, enable **When embedding a Lightning application in a third-party site, use a session token instead of a session cookie**. This setting replaces the authentication cookie with a session token when a Lightning app is in a third-party context, such as Lightning Out. Browsers are restricting the use of third-party cookies. As a result, a Lightning app that uses third-party cookies must use a different approach to maintain the session identifier between the browser and the server. This setting is an alternative to requiring that users disable browser settings, such as Safari's **Prevent cross-site tracking setting**.

Configure Secure Connections (HTTPS) Settings

By default, Salesforce requires HTTPS connections and automatically upgrades HTTP requests to HTTPS via the HSTS header. HTTPS is also required for connections to third-party domains.

1. From Setup, in the Quick Find box, enter *Session Settings*, then select **Session Settings**.
2. The **Force relogin after Login-As-User** setting is enabled by default. When this setting is enabled, an admin who is logged in as another user to log in again after logging out as the other user. For easier user activity tracking and logging, we recommend you keep this setting enabled.
3. To restrict session ID cookie access, select **Require HttpOnly attribute**. A cookie with the HttpOnly attribute isn't accessible through non-HTTP methods, such as calls from JavaScript.

 **Note:** If you have a custom or packaged application that uses JavaScript to access session ID cookies, selecting the Require HttpOnly attribute breaks your application. It denies the application access to the cookie. Also if you select this setting, the AJAX Toolkit debugging window isn't available.

4. To send session information using a POST request rather than a GET request for cross-domain exchanges, select **Use POST requests for cross-domain sessions**. For example, when you use a Visualforce page, POST requests are more secure because they keep the session information in the body of the request. But if you enable this setting, sometimes embedded content from another domain, such as an image, doesn't display.

5. To restrict the IP addresses that users can gain access from to only the IP addresses defined in Login IP Ranges, select **Enforce login IP ranges on every request**.

If you enable this setting, login IP ranges are enforced on each page request, including requests from client applications. If you don't enable this setting, login IP ranges are enforced only when a user logs in. This setting affects all user profiles with login IP restrictions.

6. For **Login IP Ranges** (for Contact, Manager, Group, and Professional editions only), if you selected **Enforce login IP ranges on every request**, specify a range of IP addresses that users must log in from (inclusive). To specify a range, click **New**, and enter a Start IP Address and End IP Address to define the range, which includes the start and end values.

 **Note:** This field isn't available in Enterprise, Unlimited, Performance, and Developer Editions. In those editions, you can specify a valid Login IP Range in the user profile settings.

Configure Caching Settings

1. From Setup, in the Quick Find box, enter *Session Settings*, then select **Session Settings**.
2. To allow a user's browser to store usernames, select **Enable caching and autocomplete on login page**. If enabled, after initial login, usernames are automatically populated into the **Username** field on the login page. If the user selects **Remember me** on the login page, the username persists after the session expires or the user logs out. The username also displays on the Switcher. This setting is enabled by default.
3. To enable secure data caching in the browser, select **Enable secure and persistent browser caching to improve performance**. When selected, this setting improves page reload performance by avoiding extra round trips to the server. This setting is enabled by default.

 **Warning:** Disabling secure and persistent browser caching has a significant negative performance impact on Lightning Experience. Only disable in these scenarios.

- Your company's policy doesn't allow browser caching, even if the data is encrypted.
- During development in a sandbox or Developer Edition, you want to see the effect of any code changes without emptying the secure cache.

4. To display the Switcher when your users select their profile pictures, select **Enable user switching**. This setting also prevents your users from seeing the Switcher when they select their profile picture. This setting is enabled by default. To prevent your org from displaying in Switchers on other orgs, deselect this setting.

 **Note:** To enable the Enable user switching setting, you must also enable the Enable caching and autocomplete on login page setting.

5. To delete cached usernames only when the user explicitly logs out, select **Remember me until logout**. If the session times out, usernames display on the Switcher as inactive. So if users are on their own computer and allow a session to time out, they can select the username to reauthenticate. But if they're on a shared computer, the username is deleted immediately when the user logs out. This setting applies to all your users.

If you don't enable this setting (default), usernames are cached only while a session is active or a user selects **Remember Me**. This option isn't available for single sign-on sessions. When the session expires, the username disappears from the login page and the Switcher. Keep this setting disabled if authentication providers aren't exposed on your login page.

6. To load Lightning Experience and other apps faster by enabling Akamai's content delivery network (CDN) to serve the static content for the Lightning Component framework, select **Enable Content Delivery Network (CDN) for Lightning Component framework**. A CDN generally speeds up page load time, but it also changes the source domain that serves the files. If your company has IP range restrictions for content served from Salesforce, test thoroughly before enabling this setting. CDNs improve the load time of static content by storing cached versions in multiple geographic locations. This setting turns on CDN delivery for the static JavaScript and CSS in the Lightning Component framework. It doesn't distribute your Salesforce data or metadata in a CDN.

Cross-Site Request Forgery Protection

Salesforce is automatically protected against Cross-Site Request Forgery (CSRF) attacks. Your non-setup pages include a random string of characters in the URL parameters or as a hidden form field. With every GET and POST request, the application checks the validity of this string of characters. The application doesn't execute the command unless the value found matches the expected value.

Configure Content Security Policy Protection

1. From Setup, in the Quick Find box, enter *Session Settings*, then select **Session Settings**.
2. To override a specific security restriction on accessing email templates in Salesforce Classic from Internet Explorer, select **Override Restriction on Accessing Email Templates in Salesforce Classic Using Internet Explorer**.



Warning: We strongly recommend against enabling this setting. Internet Explorer doesn't meet Salesforce's required level of browser security protection. Enabling this setting makes your users vulnerable to malicious third-party attempts to access your data.

3. To prohibit the use of the `unsafe-inline` source for the `script-src` directive, select **Enable Stricter Content Security Policy**.

The Lightning Component framework uses Content Security Policy (CSP), the W3C standard to control the source of content that can be loaded on a page. This setting mitigates the risk of cross-site scripting attacks and is enabled by default.



Important: We strongly recommend that you keep this setting enabled. Lightning Locker and Lightning Web Security rely on this setting to provide strong security for Lightning components.

Configure Lightning Locker API Version Setting

You can temporarily set your org to use the Lightning Locker security features of a previous Salesforce release. This setting lets you quickly return your Lightning components to full functionality if a change in Lightning Locker in a new release causes your components to work incorrectly.

1. From Setup, in the Quick Find box, enter *Session Settings*, then select **Session Settings**.
2. For **Use security enhancements in API version**, select the most recent API version where the components worked correctly. When component developers have updated the components to work with the current Lightning Locker security features, return this setting to the current API version to ensure greatest protection.

For more information, see [Select the Locker API Version for an Org](#) in the *Lightning Web Components Developer Guide*.

Configure Lightning Web Security

The Lightning Component framework offers two security architectures, Lightning Locker and Lightning Web Security.

Lightning Web Security is designed to make it easier for your Lightning components to use secure coding practices and is intended to replace Lightning Locker. Lightning Web Security is being rolled out over several releases. Lightning Web Security is generally available for Lightning web components (LWC) and Aura components.

To use Lightning Web Security instead of Lightning Locker:

1. From Setup, in the Quick Find box, enter *Session Settings*, then select **Session Settings**.
2. Select **Use Lightning Web Security for Lightning web components and Aura components**.

For more information, see [Which Components Are Supported by Lightning Web Security](#) in the *Lightning Web Components Developer Guide*.

Configure Extra Protection for Your Sessions

1. From Setup, in the Quick Find box, enter *Session Settings*, then select **Session Settings**.
2. To protect sensitive information in your URLs, such as an org ID or account number, select an HTTP Referrer Policy. See [Protect Sensitive Information in Your URLs](#).
3. To protect your users from malicious URLs and phishing, specify external domains that you trust, and then choose an External Redirection setting. You can block these redirections or alert the user that the link is taking them outside the Salesforce domain. For details, see [Manage Redirections to External URLs](#) in Salesforce Help. In Lightning Experience, the warning message applies only to web tabs.

 **Note:** **Enable Content Sniffing protection** is enabled and can't be disabled. This setting helps prevent the execution of malicious files (JavaScript, Style sheet) as dynamic content by preventing the browser from inferring the MIME type from the document content. To temporarily disable this feature for issue remediation, contact Salesforce Customer Support.

Configure Session Security Levels

You can restrict access to certain types of resources based on the security level associated with the authentication method for the user's current session. By default, each login method has one of two security levels: Standard or High Assurance. You can change the session security level and define policies so that specified resources are available only to users assigned a High Assurance level.

For sensitive operations, always require a High Assurance level of security or block users. If users already have a High Assurance session after logging in, they aren't prompted to reverify their identity in the same session. This requirement applies even if you require High Assurance for these operations.

To change the security level associated with a login method, take these steps.

1. From Setup, in the Quick Find box, enter *Session Settings*, then select **Session Settings**.
2. From Session Security Levels, select the login method from the following table.
3. To move the method to the proper category, click **Add** or **Remove**.

Session Security Levels Login Methods:

Type	Default Session Security Level	Description
Username and Password	Standard	Users log in by providing a username and password on a login page.
Delegated Authentication	Standard	Users log in by providing a username and a password that is validated using a callout to a delegated authentication endpoint.

Type	Default Session Security Level	Description
Activation	Standard	Users verify their identity when accessing Salesforce from a new browser or device.
Lightning Login	Standard	Internal users log in by using Salesforce Authenticator instead of a password.
Passwordless Login	Standard	Experience Cloud users log in by providing a verification code instead of a password.
Multi-factor authentication	High Assurance	<p>Users complete a multi-factor authentication (MFA) challenge to access a resource. For example, a user must complete MFA when accessing a report that requires a High Assurance level with the Raise session level policy.</p> <p>Be careful about changing the security level of MFA to Standard. If MFA has a Standard security level, but the user profile setting, Session security level required at login, requires a High Assurance session security level, the user can't log in. User access is blocked when the High Assurance requirement isn't met.</p>
Authentication Provider	Standard	Users log in to Salesforce using their login credentials from a third-party service provider.
SAML	Standard	<p>Users are authenticated using the SAML protocol for single sign-on.</p> <p>The security level for a SAML session can also be specified using the SessionLevel attribute of the SAML assertion sent by the identity provider. The attribute can take one of two values: STANDARD or HIGH_ASSURANCE.</p>

Configure High Assurance Sessions for Reports, Dashboards, and Connected Apps

You can also set policies requiring High Assurance on reports, dashboards, and connected apps. And you can specify an action to take when the session that's used to access the resource isn't High Assurance. These actions are supported.

- Block—Prevents access to the resource by showing an insufficient privileges error.
- Raise session level—Prompts users to complete MFA. When users authenticate successfully, they can access the resource. For reports and dashboards, you can apply this action when users access reports or dashboards, or just when they export and print them.

 **Warning:** Raising the session level to High Assurance by redirecting the user to complete MFA isn't a supported action in Lightning Experience. If you enable Lightning Experience and set the High Assurance session policy requirement, Lightning Experience users with a standard session are blocked from reports and dashboards. Also, they don't see the icons for these resources in the navigation menu. As a workaround, users with a Standard Assurance session can log out and log in again using an authentication method that is defined as High Assurance for their org. Then they can access reports and dashboards. Or they can switch to Salesforce Classic, where they're prompted to raise the session level when they attempt to access reports and dashboards.

Session levels have no impact on resources in the app other than connected apps, reports, and dashboards that have defined security policies.

For information about requiring High Assurance when accessing a connected app, see [Manage Session Policies for a Connected App](#).

To require a High Assurance policy when accessing reports and dashboards, take these steps.

1. From Setup, in the Quick Find box, enter *Access Policies*, then select **Access Policies**.
2. Select **High Assurance session required**.
3. Select an option to block access to reports and dashboards or to raise the session level to high assurance.
4. Save your changes.

For more information, see [Require High Assurance Session Security for Sensitive Operations](#)

Configure Logout Page Settings

1. From Setup, in the Quick Find box, enter *Session Settings*, then select **Session Settings**.
2. For **Logout URL**, enter the URL for the page to redirect users to after they log out of Salesforce. For example, enter the URL for an authentication provider's page or a customer-branded page.

This redirect logout URL is used only if no logout URL is specified in the identity provider, SAML single sign-on, or third-party authentication provider settings. If you don't provide a logout URL, the default is `https://MyDomainName.my.salesforce.com`.
3. To redirect all expired tabs in your browser to your custom logout URL, select **Store the redirect logout URL in your local browser**. Before enabling this setting, review these considerations.

This setting uses the browser's local storage to store the custom logout URL. Verify that this setting doesn't interfere with your custom login integrations.

Configure Session Settings for New User Email

1. From Setup, in the Quick Find box, enter *Session Settings*, then select **Session Settings**.
2. For **Link expires in**, select the amount of time that the account verification link in welcome emails to new users is valid. You can select 1, 7, or 180 days. By default, account verification links expire after 7 days.

When you update this setting, the change applies to links in welcome emails that were already sent. For example, you sent a welcome email 2 days ago with the link set to expire in 7 days. If you update the setting so that links expire in 1 day, the link in the email you sent 2 days ago is no longer valid.

Enable Browser Security Settings

Browser security settings protect sensitive information and monitor SSL certificates.

Referrer URL Protection

When loading assets outside of Salesforce or navigating outside of Salesforce, the referrer header shows only Salesforce.com or Force.com rather than the entire URL. This feature eliminates the potential for a referrer header to reveal sensitive information that could be present in a full URL, such as an org ID. This feature is supported only for Chrome and Firefox.

Public Key Pinning

To detect man-in-the-middle attacks, Salesforce now monitors which SSL certificates users can see. Custom certificates aren't affected. Public key pinning is supported only for Chrome and Firefox.

HSTS (HTTP Strict Transport Security) Protection

HSTS redirects browsers to use HTTPS. It's enabled on all Salesforce and Visualforce pages and for all Experience Cloud sites and Salesforce Sites, and it can't be disabled. You can't modify the HSTS header or its values.

With HSTS enforced, the browser caches that only HTTPS can be used on the domain. The cache is saved for two years.

Set Trusted IP Ranges for Your Organization

Trusted IP Ranges define a list of IP addresses from which users can log in without receiving a login challenge for verification of their identity, such as a code sent to their mobile phone.

 **Note:**  [Who Sees What: Organization Access \(English only\)](#)

Watch how you can restrict login through IP ranges and login hours.

To help protect your organization's data from unauthorized access, you can specify a list of IP addresses from which users can log in without receiving a login challenge. However, this step doesn't restrict access entirely for users outside the Trusted IP Range. After these users complete the login challenge, usually by entering a code sent to their mobile device or email address, they can log in.

1. From Setup, in the Quick Find box, enter *Network Access*, and then select **Network Access**.

2. Click **New**.

3. Enter a valid IP address in the *Start IP Address* field and a higher IP address in the *End IP Address* field.

The start and end addresses define the range of allowable IP addresses from which users can log in, including the start and end values. If you want to allow logins from a single IP address, enter the same address in both fields.

The start and end IP addresses must be in an IPv4 range and include no more than 33,554,432 addresses (2^{25} , a /7 CIDR block).

4. Optionally, enter a description for the range. For example, if you maintain multiple ranges, enter details about the part of your network that corresponds to this range.

5. Save your changes.

 **Example:** Warren is an IT Systems specialist for a business that handles highly sensitive customer data. He uses the Security Center app to monitor the security posture for multiple Salesforce tenants. Warren can define and deploy Trusted IP ranges to selected tenants from the Security Center app. For more information, see [Define and Deploy Security Policies](#).

 **Note:** For organizations that were activated before December 2007, Salesforce automatically populated your organization's trusted IP address list in December 2007, when this feature was introduced. The IP addresses from which trusted users had already accessed Salesforce during the past six months were added.

SEE ALSO:

[Session Security](#)

[Security Implementation Guide](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions**

USER PERMISSIONS

To change network access:

- [Manage IP Addresses](#)

Control Access to Browser Features

To control whether requests to an external (non-Salesforce) server or URL can access the user's camera and microphone, enable the Permissions-Policy HTTP header. Then select when to allow access to each of these browser features.

1. From Setup, in the Quick Find box, enter *Session Settings*, and then select **Session Settings**.
2. In the Browser Feature Permissions section, select **Include Permissions-Policy HTTP header**. When this setting is disabled, all external apps and websites loaded from Salesforce can access the user's camera and microphone.
3. For Camera and Microphone, select when requests from Salesforce can access the browser feature.
 - a. For the most granular control over access to this browser feature, select **Trusted URLs Only**.
After you select this recommended setting, specify trusted URLs and the browser features that they can access from the Trusted URLs Setup page.
 - b. To grant access to this browser feature for all external apps and websites loaded from Salesforce, select **Always**.
 - c. To block access to the browser feature for all external apps and websites loaded from Salesforce, select **Never**.
If you select Never, even scripts from Salesforce domains can't access the browser feature.
4. Save your changes.

SEE ALSO:

[Manage Trusted URLs](#)

Require High-Assurance Session Security for Sensitive Operations

To secure different setup areas in your org, require a high-assurance level of security for sensitive operations, such as accessing reports and managing IP addresses. You can also block users from accessing these setup areas.

These settings apply only to users who have user permissions to access these operations. If users have a high-assurance session after logging in, they aren't prompted to verify their identity in the same session, even if you require high assurance for sensitive operations.

1. In Setup, enter *Identity* in the Quick Find box, and then click **Identity Verification**.
2. Under Session Security Level Policies, raise the session security level to high assurance, or block users.
 - Reports and Dashboards—Controls access to reports and dashboards. This setting is also available on the Reports and Dashboards Access Policies page. You can change this setting in either location.
 - Manage Encryption Keys—Controls access to the Platform Encryption page, the Certificate and Key Management Setup page, and the TenantSecret object.
 - Manage Auth. Providers—Controls access to the Auth. Providers page, the User Details Setup page, and the AuthProvider object.
 - Manage Certificates—Controls access to the Certificate and Key Management Setup page, Single Sign-On Settings Setup page, and the Certificate object.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Contact Manager, Group, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To modify session security settings:

- [Customize Application](#)

EDITIONS

Available in: all editions

USER PERMISSIONS

To modify session security settings:

- [Customize Application](#)

- Manage Connected Apps—Controls access to the Connected Apps Setup pages and the App Manager Setup page.
- Manage Data Export—Controls access to the Data Export Setup page.
- Manage IP Addresses—Controls access to the Network Access Setup page.
- Manage Login Access Policies—Controls access to the Login Access Policies Setup page.
- Manage Password Policies—Controls access to the Password Policies Setup page and profile details.
- Manage Permission Sets and Profiles—Controls access to the Permission Sets and Profile Setup pages and related objects.
- Manage Roles—Controls access to the Roles Setup page, the UserRole object, and the Role object in Metadata API.
- Manage Sharing—Controls access to the Sharing Settings Setup page, the SharingRules object, and the CustomObject's sharingModel field in Metadata API.
- Manage multi-factor authentication in API—Controls access to the VerificationHistory, TwoFactorInfo, and TwoFactorTempCode objects.
- Manage multi-factor authentication in User Interface—Controls access to the Identity Verification History Setup page and the VerificationHistory, TwoFactorInfo, and TwoFactorTempCode objects.
- Manage Users—Controls access to the Users Setup page.
- Unlock Users and Reset Passwords—Controls permission to reset passwords and unlock users on the Users Setup page.
- View Health Check—Controls access to the Health Check Setup page.

 **Note:** You can't block users from accessing the setup areas controlled by the Manage Permission Sets and Profiles or Manage Users settings.

View User Session Information on the Session Management Page

Monitor and protect Salesforce by reviewing active sessions and session details on the Session Management page in Setup. You can create custom list views, view details about a user associated with a specific session, and easily end suspicious sessions. Salesforce admins can view all active user sessions, and non-admins see only their sessions.

To access user session information, from Setup, in the Quick Find box, enter *Session Management*, and then select **Session Management**.

When you manually end a user's session by clicking the **Remove** button, the user must log in again to the organization.

 **Note:** If your org has a login flow with a concurrent user limit of 1, then instruct the user to wait a few minutes before attempting to log in again. The system needs time to periodically clear obsolete session records from memory.

Salesforce issues a session cookie to record encrypted authentication information for the duration of a specific session. The session cookie doesn't include the user's username or password. Salesforce doesn't use cookies to store other confidential user and session information, but instead implements more advanced security methods based on dynamic data and encoded session IDs.

This table contains information about the fields that you can view on this page. Because of the nature of geolocation technology, the accuracy of geolocation fields, for example, country, city, or postal code, can vary.

Field	Description
City	The city where the user's IP address is physically located. This value isn't localized.
Country	The country where the user's IP address is physically located. This value isn't localized.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: All Editions

Field	Description
Country Code	The ISO 3166 code for the country where the user's IP address is physically located. This value isn't localized. For more information, see Country Codes - ISO 3166 .
Created	The date and timestamp of when the session began.
Latitude	The latitude where the user's IP address is physically located.
Location	The approximate location of the IP address from where the user logged in. To show more geographic information, such as approximate city and postal code, create a custom view to include those fields. This value isn't localized.
Longitude	The longitude where the user's IP address is physically located.
Login Type	The type of login associated with the session. Some login types include Application, SAML, and Portal.
Parent Session ID	If a session has a parent, this ID is the parent's unique ID.
Postal Code	The postal code where the user's IP address is physically located. This value isn't localized.
Session ID	The unique ID for the session.
Session Type	The type of session the user is logged in to. For example, common ones are UI, Content, API, and Visualforce.
Source IP	The IP address associated with the session.
Subdivision	The name of the subdivision where the user's IP address is physically located. This value isn't localized.
User Type	The profile type associated with the session.
Username	The username used when logged in to the session. To view the user's profile page, click the username.
Updated	The date and timestamp of the last session update due to activity. For example, during a UI session, users make frequent changes to records and other data as they work. With each change, both the <code>Updated</code> and <code>Valid Until</code> date and timestamps are refreshed.
Valid Until	If you don't end the session manually, the date and timestamp of when the session automatically expires.

SEE ALSO:

[User Session Types](#)

User Session Types

Learn about the session types in the User Session Information page to help you monitor and protect your org.

You can view the session type for a specific user on the User Session Information page. To access the page from Setup, enter *Session Management* in the Quick Find box, then select **Session Management**.

Session types indicate the type of session a user is using to access your org. Session types can be persistent or temporary. You can access them by using the user interface, API, or other methods, such as an OAuth authentication process.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions**

Session Type	Description
API	Created when accessing an org through the API.
APIOnlyUser	Created to enable a password reset in the user interface for API-only users.
Aura	Created for access to Lightning Experience functionality.
ChatterNetworks	Created when using Chatter Networks or Chatter Sites.
ChatterNetworksAPIOnly	Created when using the Chatter Networks or Chatter Sites API.
ChatterNetworksAPIOnlyOAuth	Created when approving OAuth access by a Chatter Sites user.
Content	Created when serving user-uploaded content.
DataDownloadOnly	A session that allows users to download data when their org status is Locked, Suspended, or Hold. You can't create this session manually.
LightningContainerComponent	Created for use with Lightning container components.
LivePreview	Created to use the live preview functionality in Experience Builder.
Node	Created for NodeJS access.
OAuthApprovalUI	A session that allows access only to the OAuth approval page.
OAuth2	Created using OAuth flows. For example, if you use OAuth authentication for a connected app, this type of session is created.
SamlOAuthApprovalUi	Created when approving OAuth access during a SAML flow.
SiteStudio	Created when using the Experience Builder user interface.
SitePreview	Initiated when an internal canvas app is invoked.
STREAMING_API	Created for use by the streaming API.
SubstituteUser	Created when one user logs in as another user. For example, if an administrator logs in as another user, a SubstituteUser session is created.
UI	Created for access to the Salesforce Classic UI. Represents the core session for a login to the user interface.
UnspecifiedType	Created by an unknown source.
UserSite	Initiated when a canvas application is invoked.
Visualforce	Created to access Visualforce pages.
WDC_API	A session using the WDC API.

Temporary session types are used during the process of switching domains. For example, when you access Lightning Experience, a temporary session is created as part of that flow.

Temporary Session Type	Description
TempAuraExchange	Created to switch to the Lightning domain.

Temporary Session Type	Description
TempChatterNetworks	Created to switch to Chatter Networks or Chatter Sites.
TempContentExchange	Created to switch to the content domain, such as the user interface into which users enter their credentials.
TempLccExchange	Created to switch to the LCC domain.
TempLivepreviewExchange	Created to switch to using the live preview functionality in Experience Builder.
TempNodeExchange	Created to switch to NodeJS.
TempOAuthAccessTokenFrontdoor	Created for a user attempting to grant access to an application using the OAuth protocol.
TempSitepreviewExchange	Created to switch to using an internal canvas app.
TempSitestudioExchange	Created to switch to using the Experience Builder user interface.
TempVisualforceExchange	Created to switch to the Visualforce domain.
TempUIFrontdoor	Created to switch to the Salesforce UI.

SEE ALSO:

[View User Session Information on the Session Management Page](#)

Salesforce Platform Cookies

The Salesforce Platform uses cookies to improve functionality and accelerate processing times. By saving a user's settings, cookies can enhance the user's experience and the Salesforce Platform's performance.

Salesforce doesn't currently provide functionality for end-user cookie consent management. The platform is compatible with many existing third-party solutions. We recommend that you work with your internal IT teams or consult your implementation partners to identify the right solution for your organization's needs.

Cookies are divided into required, functional, and marketing. Functional cookies include preferences and statistics.

- **Required:** Strictly necessary to browse the website and to use its features.
- **Functional: Preferences:** Used by the website to remember choices made previously. Language settings are an example of a preference type cookie.
- **Functional: Statistics:** Used to collect information about how a website is used, including links clicked and which pages users visited.
- **Marketing:** Used to track online activity for a more personalized experience, including relevant advertisement.

 **Note:** The Salesforce Platform can run without the use of functional cookies, but doing so can reduce functionality. The impact on functionality depends on the purpose of the blocked cookie.

This table describes the Salesforce Platform cookies collected by Salesforce.

EDITIONS

Available in: All editions

Table 10: Cookies for All Users (Authenticated and Unauthenticated)

Cookie Name	Duration	Cookie Type	Description
__Host-ERIC_PROD-<random number>	1 Minute	Required	Enterprise Request Infrastructure Cookie (ERIC) carries the cross-site request forgery (CSRF) security token between the server and the client. The cookie name indicates the server mode (PROD or PRODDEBUG) and a random number. A different token is generated for each Lightning app.
_ga	2 Years	Functional: Statistics	A third-party cookie that's used if the site admin chooses to track site users with a Google Analytics tracking ID.
{UserId}_KMPage	1 Day	Functional: Preferences	In Salesforce Classic, used to read the last user selection for Find in View, Article Language, {DataCategory}, and Validation Status in Article Management.
{UserId}_KnowledgePageDispatcher	Session	Functional: Preferences	In Salesforce Classic, used to remember the user selection to determine whether to show Articles or My Drafts view in Knowledge.
{UserId}_KnowledgeFilter{DataCategory}	Session	Functional: Preferences	In Salesforce Classic, used to remember the last user selection for the data category filter in Knowledge.
{UserId}_KnowledgeFilterArticleType	Session	Functional: Preferences	In Salesforce Classic, used to remember the last user selection for the article type filter for Articles view in Knowledge.
{UserId}_KnowledgeFilterArticlePublishStatus	Session	Functional: Preferences	In Salesforce Classic, used to remember the last user selection for the publish status filter for Articles view in Knowledge.
{UserId}_KnowledgeFilterArticleValidationStatus	Session	Functional: Preferences	In Salesforce Classic, used to remember the last user selection for the validation status filter for Articles view in Knowledge.
{UserId}_KnowledgeFilterLanguage	Session	Functional: Preferences	In Salesforce Classic, used to remember the last user selection for the language filter in Knowledge.
{UserId}_KnowledgeFilterMyDraftArticleType	Session	Functional: Preferences	In Salesforce Classic, used to remember the last user selection for

Cookie Name	Duration	Cookie Type	Description
			the article type filter for My Drafts view in Knowledge.
{User Id}_KnowledgeItemDraftPublStatus	Session	Functional: Preferences	In Salesforce Classic, used to remember the last user selection for the publish status filter for My Drafts view in Knowledge.
{User Id}_KnowledgeItemDraftValidStatus	Session	Functional: Preferences	In Salesforce Classic, used to remember the last user selection for the validation status filter for My Drafts view in Knowledge.
{User Id}_KnowledgePageSortFieldArticle	Session	Functional: Preferences	In Salesforce Classic, used to remember the last user selection for Sort by for the Articles view in Knowledge.
{User Id}_KnowledgePageSortFieldDraft	Session	Functional: Preferences	In Salesforce Classic, used to remember the last user selection for Sort by for the My Drafts view in Knowledge.
{User Id}_spring_KMAyoneDraftArticlesList	1 Day	Required	In Salesforce Classic, used to configure layout properties for the Draft Articles view in Article Management.
{User Id}_spring_KMArchiveArticlesList	1 Day	Required	In Salesforce Classic, used to configure layout properties for Archived Articles in Article Management.
{User Id}_spring_KMMDraftArticlesList	1 Day	Required	In Salesforce Classic, used to configure layout properties for Draft Articles assigned to Me in Article Management.
{User Id}_spring_KMMDraftTranslationsList	1 Day	Required	In Salesforce Classic, used to configure layout properties for Draft Translations in Article Management.
{User Id}_spring_KMPublishArticlesList	1 Day	Required	In Salesforce Classic, used to configure layout properties for Published Articles in Article Management.
{User Id}_spring_KMPublishTranslationsList	1 Day	Required	In Salesforce Classic, used to configure layout properties for Published Translations in Article Management.

Cookie Name	Duration	Cookie Type	Description
<namespace>_sid	Session	Required	Identifies a Live Agent session. Stores a unique pseudonymous ID for a specific browser session over chat service.
52609e00b7ee307e	Session	Required	Browser Fingerprint cookie. Used to detect session security problems.
79eb100099b9a8bf	Session	Required	Browser Fingerprint trigger cookie. Used to detect session security problems.
activeView	Session	Functional: Preferences	In Salesforce Classic, used to remember the last user selection for Articles or Translations tab in Article Management.
apex__EmailAddress	1 Year	Required	Caches contact IDs associated with email addresses.
auraBrokenDefGraph	1 Week	Functional: Statistics	Used to track when a Lightning page has malformed HTML.
autocomplete	60 Days	Functional: Preferences	Determines if the login page remembers the user's username.
BAYEAX_BROWSER	Expired on Creation	Required	Identify a unique browser subscribed to CometD streaming channels.
BrowserId	1 Year	Required	Used for security protections.
BrowserId_sec	1 Year	Required	Used for security protections.
calViewState	Session	Functional: Statistics	Sets the inline calendar date state in Salesforce Classic (current week selected).
caPanelState	Session	Functional: Preferences	Saves the open, closed, and height percent states of the calendar panel.
clientSrc	Session	Required	Used for security protections.
CookieConsent	1 Year	Required	Used to apply end-user cookie consent preferences.
CookieConsentPolicy	1 Year	Required	Used to apply end-user cookie consent preferences set by our client-side utility.
cookieSettingVerified	Session	Required	Used to create a popup message telling users that cookies are required.
cordovaVersion	Session	Required	Used for internal diagnostics with mobile applications.

Cookie Name	Duration	Cookie Type	Description
cqcid	1 Year	Functional: Statistics	Used to track a guest shopper's browsing activity.
csssid	Session	Required	Used to establish a request context in the correct tenant org.
csssid_Client	Session	Required	Enables user switching.
devOverrideCsrfToken	Session	Required	CSRF Token.
disco	Session	Required	Tracks the last user login and active session for bypassing login. For example, OAuth immediate flow.
FedAuth	Session	Required	For the SharePoint connector, used to authenticate to the top-level site in SharePoint.
force-proxy-stream	3 Hours	Required	Ensures that client requests hit the same proxy hosts and are more likely to retrieve content from cache.
force-stream	180 Minutes	Required	Used to redirect server requests for sticky sessions.
gTalkCollapsed	1 Year	Required	Controls whether the sidebar in Salesforce Classic is open for a user.
guest_uid_essential_<15-char SiteID>	1 Year	Required	Provides a unique ID for guest users in Salesforce Sites. Expires 1 year after the user's last visit to the site.
hideDevelopmentTools	Session	Functional: Preferences	Used to determine whether to show the developer tools.
hideFilesWarningModal	50 Years	Functional: Preferences	Stores the user acknowledgment that a public link to a Salesforce file is on email send. The warning window isn't continually shown after the user acknowledges this action.
hideIdentityDialog	1 Year	Functional: Preferences	Hides the dialog box that informs that the current user is logged out when switching to another user.
idccsrf	Session	Required	Tracks <code>CrossSiteRequestForgery</code> validation for certain single sign-on (SSO) flows.
ideaToggle	Session	Functional: Preferences	Show the Ideas list view or the Feed list view.

Cookie Name	Duration	Cookie Type	Description
inst	Session	Required	Used to redirect requests to an instance when bookmarks and hardcoded URLs send requests to a different instance. This type of redirect can happen after an org migration, a split, or after any URL update.
iotcontextsplashdisable	10 Years	Functional: Preferences	For the IoT product, stores user preference of whether to show Context Splash popup.
language	Session	Required	Identifies the language for custom components, surveys, and flows, which support multiple languages. Without this cookie, translations for custom features can appear incorrectly.
lastlist	Session	Required	Used to store the cookie name for the last list URL.
liveagent_invite_rejected_	Session	Functional: Statistics	Instructs Live Agent not to reissue an invitation on the same domain. Deletion of this cookie degrades the customer's experience because they can get repeated invitations.
liveagent_sid	Session	Required	Identifies a Live Agent session. Stores a unique pseudonymous ID for a specific browser session over chat service.
lloopch_loid	1 Year	Required	Determines whether to send the user to a specific portal login or an app login.
login	60 Days	Functional: Preferences	If the user's session has expired, used to fetch the username and populate it on the main login page when using the process builder app.
oinfo	3 Months	Functional: Statistics	Tracks the last logged in org.
pc-unit	1 Year	Functional: Preferences	Sets a preference for displaying platform cache units to either MB or KB.
PreferredLanguage	1 Year	Functional: Preferences	Stores the user language preference for language detection and localized user experience.

Cookie Name	Duration	Cookie Type	Description
promptTestMod	30 Days	Required	Stores whether test mode is in effect. This cookie is read-only.
redirectionWarning	1 Year	Functional: Preferences	Enables the customer to store URLs that are exempt from setting a redirect warning interstitial page on an allowlist.
RRetURL	Session	Required	Used with Log in As to restore the original state.
RRetURL2	Session	Required	The return URL to redirect to when logging out of a session.
RSID	Session	Required	Session ID and login as session ID. In this case, the cookies are copied to the response and cause the target URL to rebuild appropriately in a proxy situation. The cookies aren't created, examined, or modified.
schgtclose	0	Functional: Statistics	Deprecated feature, not used.
sfdc_lv2	1 Year	Required	Stores device activation details for users. If the cookie isn't set or it expires, users must verify their identity the next time that they log in. Identity verification requires a verification method such as SMS, an authenticator app, or a security key.
sfdc-stream	3 hours	Required	Used to properly route server requests within Salesforce infrastructure for sticky sessions.
showNewBuilderWarningMessage	100 years	Functional: Preferences	Used to show or hide a warning message for the new dashboard builder.
sid	Session	Required	The Session ID used to authenticate Lightning Platform Soap-API and Rest-API data connections for the current user.
sid_Client	Session	Required	Used to detect and prevent session tampering.
sidebarPinned	10 Years	Required	Controls the state of the Salesforce Classic sidebar.
ssostartpage	1 Year	Required	Identifies the Identity Provider (IdP) location for single sign-on (SSO).

Cookie Name	Duration	Cookie Type	Description
			Certain service provider initiated SSO requests can fail without this cookie.
SUCSP	Session	Required	Used when the user identity that an administrator is assuming, via Log In as Another User, is a Customer Success Portal (CSP) user.
SUPRM	Session	Required	Used when the user identity that an administrator is assuming, via Log In as Another User, is a Partner Relationship Management (PRM) portal user.
t	Expired on Creation	Functional: Statistics	Used to avoid duplicate access checks.
useStandbyUrl	Not Set	Required	Controls how quickly to set the standby URL when loading the softphone.
waveUserPrefFinderLeftNav	100 Years	Functional: Preferences	Preference for left navigation UI in CRM Analytics.
waveUserPrefFinderListView	100 Years	Functional: Preferences	Preference for displaying list views in CRM Analytics.
webact	1 Year	Functional: Statistics	Used to collect metrics per page view for personalization.
WelcomePanel	1 Day	Functional: Preferences	Stores Salesforce preferences.

Using Frontdoor.jsp to Bridge an Existing Session Into Salesforce

You can use `frontdoor.jsp` to give users access to Salesforce from a custom web interface, such as a Salesforce site, using their existing session ID and the server URL.

To authenticate users with `frontdoor.jsp`, you must parse the session ID (not just the 15-character or 18-character ID) and the instance or domain from the `serverUrl` of the `LoginResult` returned from SOAP API `login()` call. We recommend passing these values to `frontdoor.jsp` through a form that uses a `POST` request.

 **Note:** Users with the API Only User permission can use bridged sessions only to change and reset their passwords. They can't access any other UIs.

For example, the following form posts the current session ID to `frontdoor.jsp`.

```
<form method="POST" action="https://domain_name/secur/frontdoor.jsp">
<input type="hidden" name="sid"
    value="full_sessionID_value" />
<input type="hidden" name="retURL"
```

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions**

```
value="optional_relative_url_to_open" />
<input type="submit" name="login" value="Log In" /></form>
```

In this example, `domain_name` is the domain of the server URL (for example, `myDomainName.my.salesforce.com`).

OAuth 2.0 Hybrid App Token Flows

For OAuth 2.0 hybrid app token flows, the hybrid app sets the domains' associated SIDs in the session cookies to directly bridge a web session without using `frontdoor.jsp`.

For web sessions that are resetting user division on objects for the Reset to Default Division on Login setting, the hybrid app must bridge a web session using `frontdoor.jsp`. You can bypass session interruptions that occur with the standard `frontdoor.jsp` flow. Make a `POST` request to `frontdoor.jsp` with the value `directBridge2=true`. The `directBridge2` parameter directly passes the access token to the session ID cookie of the requested domain. With this flow, the hybrid app uses the same access token for API calls and UI requests, so remembering when your access and refresh tokens expire is unnecessary.

Make sure that the session ID value is an OAuth 2.0 access token with web scope and that it's passed in the `POST` body, not a query string. The mobile app must use the OAuth 2.0 hybrid app token flows and be able to manage session cookies in web view. The `directBridge2` parameter isn't supported in standard web browsers.

For more information, see [OAuth 2.0 Authorization and Session Management for Hybrid Apps](#).

Full Session ID

An example of a full session ID is the `access_token` obtained from OAuth authentication. One of the scopes specified when you create a connected app must be `web` or `full`.

 **Note:** Not all session types are supported with `frontdoor.jsp`, such as Experience Cloud site API sessions. For these sessions, consider using SAML for single sign-on, instead.

You have several ways to get a Session ID, such as from `UserInfo.getSessionId()` in Apex, `$Api.SessionID` and other sources. Sometimes the ID values from these sources vary depending on context, don't work with `frontdoor.jsp`, and can pose security risks as you use them. Use the `access_token` from an OAuth authentication for a secure, reliable value.

Relative URL to Open

You can optionally include a URL-encoded relative path to redirect users to the Salesforce user interface or a particular record, object, report, or Visualforce page, for example, `/apex/MyVisualForcePage`.

Secure Cross-Cloud Integrations with Private Connect

When you integrate your Salesforce org with applications hosted on third-party cloud services, it's essential to be able to send and receive HTTP/s traffic securely. With Private Connect, increase security on your Amazon Web Services (AWS) integrations by setting up a fully managed network connection between your Salesforce org and your AWS Virtual Private Cloud (VPC). Then, route your cross-cloud traffic through the connection instead of over the public internet to reduce exposure to outsider security threats.

Private Connect is available in partnership with AWS via a feature called AWS PrivateLink. PrivateLink provides private connectivity between VPCs, AWS services, and on-premise applications on the Amazon Network. Connect your existing or new AWS VPC to a Salesforce-managed VPC with PrivateLink. Then, all the data traffic flowing between your VPC and your Salesforce org is automatically routed through the connection.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise, Performance, Unlimited, and Developer** Editions

Private Connect is also bi-directional: you can initiate both inbound and outbound traffic. With inbound connections, you can send traffic into Salesforce using the standard APIs. And with outbound connections, you can send traffic out of Salesforce via features like Apex callouts, External Services, and External Objects.

Private Connect is available for purchase as an add-on license. Read the Considerations documentation to see if you can add Private Connect to your org.

Overview of Inbound and Outbound Connections with AWS

	Inbound	Outbound
Description	Data traffic flows from AWS to Salesforce	Data traffic flows from Salesforce to AWS
Salesforce Prerequisites	My Domain	Named Credentials
AWS VPC Prerequisites	<ul style="list-style-type: none"> • VPC • VPC Endpoint • Route53 	<ul style="list-style-type: none"> • VPC • VPC Endpoint Service

[Establish an Inbound Connection with AWS](#)

An inbound connection allows you to send traffic into Salesforce from your AWS Virtual Private Cloud (VPC) using the standard APIs.

[Establish an Outbound Connection with AWS](#)

An outbound connection allows you to send traffic from Salesforce to your AWS Virtual Private Cloud (VPC) using Named Credentials.

[Considerations for Private Connect with AWS](#)

Before provisioning an inbound or outbound connection with an AWS VPC, check the current limitations of the feature.

Establish an Inbound Connection with AWS

An inbound connection allows you to send traffic into Salesforce from your AWS Virtual Private Cloud (VPC) using the standard APIs.

Overview

From the AWS Regions dropdown in the Private Connect Setup page, copy the Service Name that corresponds to your AWS VPC region. In AWS, use the Service Name to create an Endpoint for your VPC. Then, use the VPC Endpoint ID of the newly created Endpoint to create an Inbound Connection in the Setup wizard. Use Route53 as a private Hosted Zone to map your VPC to your Salesforce My Domain so that all traffic is redirected over the connection. Provision the connection when you're ready to use it and continue to call the standard Salesforce APIs.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise, Performance, Unlimited, and Developer** Editions

The screenshot displays the Salesforce Private Connect Setup page. At the top, there is a 'SETUP Private Connect' header. Below it, the 'AWS Regions' section contains a table with columns for Region, IAM Role, and Service Name. The 'Inbound Connections' section features a table with columns for Private Connection Name, Description, Region, VPC Endpoint Id, Private Connection Status, and Actions. The 'Outbound Connections' section also has a table with similar columns, including Service Name. Each section includes a 'Create' button.

1. From Setup, in the Quick Find box, enter *Private Connect*, and then select **Private Connect**.
2. To open a dropdown menu of the available regions, IAM Roles, and Service Names, click **AWS Regions**.
3. Find the region in which your VPC is hosted and copy the corresponding **Service Name**.
4. In the AWS Console, create an Endpoint using the Service Name you copied in Step 3 for your VPC.
5. After saving the Endpoint, copy the VPC Endpoint ID and the IP address from the Subnet of your Endpoint.
6. From the Private Connect Setup page, click **Create Inbound Connection**.
7. Select the **AWS PrivateLink** Connection Type.
8. Enter the Connection Name, Description, and the VPC Endpoint ID you copied in Step 5.
9. Save your changes. Your connection appears on the Inbound Connections list with the Status field as Unprovisioned.
10. In the AWS Console, create a private Hosted Zone with your My Domain name and the VPC ID that matches the location of the endpoint. Create a Record Set for the Hosted Zone that includes your My Domain name and the IP address of your Endpoint Subnet from Step 5.
To ensure that your Hosted Zone and Record Set are configured properly, perform an `nslookup` of your My Domain from your VPC. Make sure it matches the Record Set entry in the Hosted Zone and not the public Salesforce IP.
11. From the Private Connect Setup page, click the arrow under the Actions field that corresponds to your connection on the Inbound Connections list. Click **Sync**.



Warning: After the Status field changes to Ready, it can take an extra few minutes for the connection to be fully prepared for runtime callouts. Wait a few minutes before making callouts.

To view details about the inbound connection, such as its allocated source IP addresses, click the connection name. Use these IP addresses to further [protect your Salesforce org.](#) on page 1055

Managing your connection:

- If you update a developer-controlled field of a private connection during a package upgrade (service name, endpoint ID, or region) you risk breaking the connection.
- If you delete an inbound connection in Salesforce, you must delete the endpoint in AWS as well.

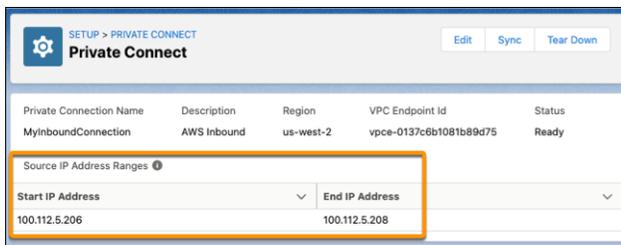
- If you make any external changes to a connection, Sync the connection in Salesforce to retrieve the latest status or catch runtime errors.

Note: The Status field is programmatically controlled. When it's Unprovisioned, the Actions field allows you to Edit, Provision, and Delete the connection. After you click Provision, the field automatically moves through the in-between states until it gets to Ready. When the status is Provisioned, the Actions field allows you to Edit, Sync, and Teardown the connection. Only connections with a Ready status can send traffic. The following are the possible values for the Status field:

- Unprovisioned
- Allocating
- PendingAcceptance
- PendingActivation
- RejectedRemotely
- DeletedRemotely
- TeardownInProgress
- Ready

Use Source IP Addresses For Added Security

The Source IP Address Ranges table on an inbound connection's detail page lists the IP addresses allocated to the connection.



Private Connection Name	Description	Region	VPC Endpoint Id	Status
MyInboundConnection	AWS Inbound	us-west-2	vpc-e-0137c6b1081b89d75	Ready

Start IP Address	End IP Address
100.112.5.206	100.112.5.208

These IP address ranges are allocated by the Salesforce-managed VPC in your cloud provider, such as AWS. The IP addresses are unique to your inbound connection and don't change after you provision it. Use them to add more protection to your Salesforce org. Here are some examples.

- Define a list of IP addresses that users can log in from without receiving a login challenge.
- Restrict the IP addresses that users can access Salesforce from to only certain ranges.
- Let Salesforce Authenticator automatically verify identities based on trusted IP addresses only.
- Monitor and view the user session information about Private Connect users, including their source IP address.
- View the login history of Private Connect users, including their source IP address.
- Control login access at the user level by specifying a range of allowed IP addresses on a user's profile.
- Restrict access to trusted IP address when using the OAuth web server flow.

SEE ALSO:

[Modify Session Security Settings](#)

[View User Session Information on the Session Management Page](#)

Establish an Outbound Connection with AWS

An outbound connection allows you to send traffic from Salesforce to your AWS Virtual Private Cloud (VPC) using Named Credentials.

Overview

From the AWS Regions dropdown in the Private Connect Setup page, copy the IAM Role that corresponds to your AWS VPC region. In AWS, add the copied IAM Role to the Whitelisted Principals tab of the VPC Endpoint Service you want to connect to. Then, copy the Endpoint Service DNS Name, and use it to create an Outbound Connection in the Setup wizard within Salesforce. Provision the connection when you are ready to use it. Register your endpoint URL within a Named Credential, and reference the Outbound Connection using the new `OutboundNetworkConnection` field. All callouts from Salesforce using this Named Credential are routed through the private connection.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise, Performance, Unlimited, and Developer** Editions

The screenshot shows the Salesforce Private Connect Setup interface. At the top, there's a 'SETUP Private Connect' header. Below it, the 'AWS Regions' section is expanded, showing a table with columns for Region, IAM Role, and Service Name. Two rows are visible: 'us-east-1' with 'Region information is temporarily unavailable' for both IAM Role and Service Name, and 'us-west-2' with 'arn.aws.iam::325178561262:role/us-west-2-private-connect' for IAM Role and 'com.amazonaws.vpce.us-west-2.vpce-svc-051704a4147764fc3' for Service Name. Below this, the 'Inbound Connections' section has a 'Create Inbound Connection' button and a table with columns: Private Connection Name, Description, Region, VPC Endpoint Id, Private Connection Status, and Actions. One row is shown for 'inbound' in 'us-west-2' region with VPC Endpoint Id 'vpce-0bb9a8b61c3ae460e' and status 'Unprovisioned'. The 'Outbound Connections' section has a 'Create Outbound Connection' button and a table with columns: Private Connection Name, Description, Region, VPC Endpoint Id, Service Name, Private Connection Status, and Actions. One row is shown for 'Outbound' in 'us-west-2' region with VPC Endpoint Id 'vpce-00dee9a0bc4a4abee', Service Name 'com.amazonaws.vpce.us-west-...', and status 'Ready'.

1. From Setup, enter *Private Connect* in the Quick Find box, and then select **Private Connect**.
2. To open a dropdown menu of the available regions, IAM Roles, and Service Names, click **AWS Regions**.
3. Find the region in which your VPC is hosted, and copy the corresponding **IAM Role**.
4. In the AWS Console, add the IAM Role to the Whitelisted Principals tab of your VPC Endpoint Service. This grants AWS access to the Salesforce-managed VPC.
5. After saving the Endpoint Service, copy the VPC Endpoint Service Name and the DNS Name of the Endpoint Service's Network Load Balancer.
6. From the Private Connect Setup page, click **Create Outbound Connection**.
7. Select the **AWS PrivateLink** Connection Type.
8. Enter the Connection Name, Description, and the VPC Endpoint Service Name you copied in Step 5.
9. Save your changes. Your connection appears on the Outbound Connections list with the Status field as Unprovisioned.
10. Click the arrow under the Actions field that corresponds to your connection on the Outbound Connections list. Click **Sync**.



Warning: After the Status field changes to Ready, it can take an extra few minutes for the connection to be fully prepared for runtime callouts. Wait up to 5 minutes before making callouts.

11. Register your AWS VPC Endpoint Service Name as a Named Credential using the new `OutboundNetworkConnection` lookup field. Make sure that the hostname matches the certificate of the endpoint service.

 **Note:** The URL should contain the VPC Endpoint Service DNS Name from Step 5 and the port of the destination service, separated by a colon. If your target group is attached to a port that is different than the default for the protocol, you must specify the port in the URL. An HTTP URL defaults to Port 80 and an HTTPS URL defaults to port 443.

Managing your connection:

- If you update a developer-controlled field of a private connection during a package upgrade, such as service name, endpoint ID, or region, you risk breaking the connection.
- If you make any external changes to a connection, Sync the connection in Salesforce to retrieve the latest status or catch runtime errors.

 **Note:** The Status field is programmatically controlled. When it is Unprovisioned, the Actions field allows you to Edit, Provision, and Delete the connection. After you click Provision, the field automatically moves through the in-between states until it gets to Ready. When the status is Provisioned, the Actions field allows you to Edit, Sync, and Teardown the connection. Only connections with a Ready status can send traffic. The following are the possible values for the Status field:

- Unprovisioned
- Allocating
- PendingAcceptance
- PendingActivation
- RejectedRemotely
- DeletedRemotely
- TeardownInProgress
- Ready

Considerations for Private Connect with AWS

Before provisioning an inbound or outbound connection with an AWS VPC, check the current limitations of the feature.

Required User Permissions

Users who aren't admins can modify inbound and outbound Private Connections using the Tooling, Metadata, and Connect APIs. They can also use third-party tools that are built on these APIs, such as Amazon AppFlow. But before users can use these APIs or tools to modify Private Connections, they must be assigned these user permissions.

- Allow user to modify Private Connections
- Modify Metadata Through Metadata API Functions

Enable these user permissions by creating or modifying a [permission set](#) and assigning it to the user. In Setup, these permissions are listed in the System Permissions section of the Permission Sets page. Creating a separate permission set with these permissions is useful for users who use third-party tools to modify Private Connections but don't need other administrative permissions.

Current Availability

AWS Regions

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

AWS Region	Location
ap-northeast-1	Tokyo, Japan
ap-northeast-2	Seoul, South Korea
ap-south-1	Mumbai, India
ap-southeast-1	Singapore
ap-southeast-2	Sydney, Australia
ap-southeast-3	Jakarta, Indonesia
ca-central-1	Montreal, Canada
eu-central-1	Frankfurt, Germany
eu-north-1	Stockholm, Sweden
eu-south-1	Milan, Italy
eu-west-2	London, United Kingdom
eu-west-3	Paris, France
sa-east-1	São Paulo, Brazil
us-east-1	Northern Virginia, USA
us-west-2	Oregon, USA

 **Note:** The AWS Regions dropdown in the Private Connect Setup page shows only the regions that your Salesforce org can access. If you don't see your VPC region in the dropdown, you can peer your existing VPC to an available region that shows in the dropdown. You can also create a VPC inside an available region before creating a connection.

Supported Salesforce Services

- Experience Cloud
- Financial Services Cloud
- Health Cloud
- Platform Cloud
- Sales Cloud
- Service Cloud

 **Note:** Private Connect also supports AppExchange Partners on each of the listed clouds.

Supported Salesforce Features

- Inbound: All supported public APIs
- Outbound: Apex Callouts, External Services, Salesforce Connect Custom Adapter, OData 4.01 adapter for Salesforce Connect, Salesforce Connect SQL adapter for Amazon Athena, Platform Events, Change Data Capture

Unsupported Salesforce Feature

- [Locked sessions to the IP address from which they originated](#)

Licensing

Each Private Connect license allows for one provisioned connection in each direction, inbound and outbound. Each connection represents a one-to-one mapping between an org ID and a VPC Endpoint ID. Every provisioned connection requires a Private Connect license. For example, four inbound connections require four licenses, leaving four available outbound connections.

There's a per-org limit of 1,000 connections per direction. Connections in an unprovisioned state don't count toward your license.

Rate Limits

The data rate limit is managed on an hourly basis. Data doesn't roll over after an hour or accumulate. Rate limits are managed separately for inbound connections and outbound connections.

- Inbound connections are used by tools like MuleSoft or Amazon AppFlow to call in to the standard enterprise APIs.
- Outbound connections are used by Apex code or platform tools like Flow and External Services to fetch data from external systems.

The initial license purchase entitles the org to 225 MB of data per hour. Usage is expressed in hourly terms because the [Limits API](#) allows you to track the remaining outbound allocation on a per-hour basis. Standard enterprise API limits apply to inbound connections.

Contact Salesforce to purchase a separate add-on license for more data. Outbound connections can't transfer more than 56.48 GB of data per hour.

Direction	Default Rate Limit Per Org Per Hour	Max Rate Limit Per Org Per Hour
Inbound	225 MB	56.48 GB
Outbound	225 MB	56.48 GB

Sandbox, Scratch Org, and Developer Org Limitations

Environment	Limitations
Full and Partial Copy Sandboxes	Private connections aren't copied from production orgs and must be recreated in sandbox environments. You can create and provision connections.
Developer and Developer Pro Sandboxes	Private connections aren't copied from production orgs and must be recreated in sandbox environments. You can create connections, but you can't provision them.
Scratch Orgs	You can create connections, but you can't provision them.
Developer Orgs	You can create connections, but you can't provision them unless you file a case.

Standards Compliance

Private Connect maintains compliance with these standards:

- ISO 27001, 27017, 27018
- SOC 2 Type II
- ASIP Santé HDS
- NEN 7510

- PCI-DSS

If you want to build Health Care applications on Salesforce that comply with the US Health Insurance Portability and Accountability Act (HIPAA), contact your account representative about signing a Business Associate Addendum.

See [Compliance engineered for the Cloud](#) for more information about these standards.

SEE ALSO:

[Knowledge Article: Troubleshoot and fix Salesforce Private Connect inbound connection issues](#)

Activations

Activation tracks information about devices from which users have verified their identity. Salesforce prompts users to verify their identity when they access Salesforce from an unrecognized browser or application. Identity verification adds an extra layer of security on top of username and password authentication. The Activations page lists the login IP addresses and client browsers used.

When a user logs in from outside a trusted IP range and uses a browser or app we don't recognize, the user is challenged to verify identity. We use the highest-priority verification method available for each user. In order of priority, the methods are:

1. Verification via push notification or location-based automated verification with the Salesforce Authenticator mobile app (version 2 or later) connected to the user's account.
2. Verification via a U2F security key registered with the user's account.
3. Verification code generated by a mobile authenticator app connected to the user's account.
4. Verification code sent via SMS to the user's verified mobile phone.
5. Verification code sent via email to the user's email address.

After identity verification is successful, the user doesn't have to verify identity again from that browser or app, unless the user:

- Manually clears browser cookies, sets the browser to delete cookies, or browses in private or incognito mode
- Deselects **Don't ask again** on the identity verification page

The Activations page in Setup lists the login IP addresses and client browser information of devices from which users have verified their identity. You can revoke the browser activation status for one, many, or all users.

For example, a user reports a lost device and is issued a new one. You can revoke the activation status of the browser on the lost device so that anyone attempting to access the org from that device has to verify their identity. This identity verification adds a layer of security while allowing users to stay productive.

Users can view their own Activations page to check their login IP addresses and client browser information. End users can revoke the activation status only for their own activated browsers.

For example, a user logs in to the org. On the user's Activations page, several different browsers are activated, but the user has only logged in from a single browser on a work laptop. The user immediately revokes the activation status of those browsers the user doesn't recognize. Because this user is challenged for identity verification using a code sent via SMS to the user's mobile device, anyone else who tries to log in from one of the deactivated browsers can't get the texted verification code. Without the code, the hacker fails the identity verification challenge. The user can then report the potential security breach.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

Available in: **All Editions**

[Use Activations](#)

View your users' activations and revoke activation status to prevent security breaches.

SEE ALSO:

[Use Activations](#)

Use Activations

View your users' activations and revoke activation status to prevent security breaches.

To see login IP and browser information about devices from which users have verified their identity, from Setup, enter *Activations* in the **Quick Find** box, then select **Activations**.

You can revoke activation status by selecting one or more entries in the Activated Client Browser list, clicking **Remove**, and confirming the action. Users can view and revoke only their own activated browsers. A user who logs in from a deactivated browser is prompted to verify identity, unless the login IP address is within a trusted IP range.

 **Note:** When a user deselects the **Don't ask again** option that appears on the identity verification page, the browser isn't activated. Advise your users to deselect this option whenever they log in from a public or shared device.

SEE ALSO:

[Activations](#)

Real-Time Event Monitoring

Real-Time Event Monitoring helps you monitor and detect standard events in Salesforce in near real-time. You can store the event data for auditing or reporting purposes. You can create transaction security policies using Condition Builder—a point-and-click tool—or Apex code.

With Real-Time Event Monitoring, gain greater insights into:

- Who viewed what data and when
- Where data was accessed
- When a user changes a record using the UI
- Who is logging in and from where
- Who in your org is performing actions related to Platform Encryption administration
- Which admins logged in as another user and the actions the admin took as that user
- How long it takes a Lightning page to load
- Threats detected in your org, such as anomalies in how users view or export reports, session hijacking attacks, or credential stuffing attacks

As a best practice, before creating transaction security policies, you can view or query events to determine appropriate thresholds for normal business usage.

[Real-Time Event Monitoring Definitions](#)

Keep these terms in mind when working with Real-Time Event Monitoring.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions**

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer Editions**

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

[Considerations for Using Real-Time Event Monitoring](#)

Keep the following considerations in mind as you set up and use Real-Time Event Monitoring.

[Enable Access to Real-Time Event Monitoring](#)

You can set user access to Real-Time Event Monitoring through profiles and permission sets.

[Stream and Store Event Data](#)

Explore how you can use the objects in Real-Time Event Monitoring to stream and store event data.

[Create Logout Event Triggers](#)

If the LogoutEventStream object is available to your org, you can create Apex triggers that respond to security logout events from your org's UI.

[How Chunking Works with ReportEvent and ListViewEvent](#)

Chunking occurs when a report or list view execution returns many records and Salesforce splits the returned data into chunks.

[Enhanced Transaction Security](#)

Enhanced Transaction Security is a framework that intercepts real-time events and applies appropriate actions to monitor and control user activity. Each transaction security policy has conditions that evaluate events and the real-time actions that are triggered after those conditions are met. The actions are Block, Multi-Factor Authentication, and Notifications. Before you build your policies, understand the available event types, policy conditions, and common use cases. Enhanced Transaction Security is included in Real-Time Event Monitoring.

[Threat Detection](#)

Threat Detection uses statistical and machine learning methods to detect threats to your Salesforce org. While Salesforce identifies these threats for all Salesforce customers, you can view the information in the events with Threat Detection in Event Monitoring and investigate further if necessary.

[Explore Event Log File Data using the Event Log File Browser \(Beta\)](#)

The Event Log File Browser (beta) in Setup gives you quick access to event log files so you can explore and download all of your Event Log File data.

SEE ALSO:

[Salesforce Help: What's the Difference Between the Salesforce Events?](#)

[Learning Map: Shield Learning Map](#)

Real-Time Event Monitoring Definitions

Keep these terms in mind when working with Real-Time Event Monitoring.

Event

An event is anything that happens in Salesforce, including user clicks, record state changes, and measuring values. Events are immutable and timestamped.

Event Channel

A stream of events on which an event producer sends event messages and event consumers read those messages.

Event Subscriber

A subscriber to a channel that receives messages from the channel. For example, a security app is notified of new report downloads.

Event Message

A message used to transmit data about the event.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Event Publisher

The publisher of an event message over a channel, such as a security and auditing app.

Considerations for Using Real-Time Event Monitoring

Keep the following considerations in mind as you set up and use Real-Time Event Monitoring.

Salesforce Classic versus Lightning Experience

Some events apply only to Salesforce Classic or Lightning Experience.

The following objects support only Salesforce Classic:

- URISession
- URISessionStream

The following object supports only Lightning Experience:

- LightningUriSession
- LightningUriSessionStream

 **Note:** Real-Time Event Monitoring objects sometimes contain sensitive data. Assign object permissions to Real-Time Events accordingly in profiles or permission sets.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Enhanced Transaction Security

- With Enhanced Transaction Security, you can create policies using either Condition Builder or Apex code.
- Enhanced Transaction Security policies support both standard and custom objects.
- The multi-factor authentication action isn't available in the Salesforce mobile app, Lightning Experience, or via API for any events. Instead, the block action is used. For example, if a multi-factor authentication policy is triggered on a list view performed via the API, Salesforce blocks the API call.
- A value of 0 for the `RowsProcessed` field in an object (such as `ApiEvent`) indicates that a query was performed and nothing was returned. This scenario is possible if a user doesn't have the correct permissions for a data row or the query doesn't return results. In this case, the `QueriedEntities` field is empty.
- Let's say you create both an Apex and a Condition Builder policy on the same event. You also specify the same action (Block or multi-factor authentication) for both policies. In this case, the Apex policy executes before the Condition Builder policy. The `PolicyId` field of the event reflects the last policy that was executed and triggered.
- You can't use the same Apex class on policies with the same event. When you create an Apex policy using Condition Builder, the list of available Apex classes can differ based on the policies you already created.
- Let's say you enable a transaction security policy for an event in which the action is None. As a result, when an event satisfies the policy conditions, the policy isn't triggered. However, these event fields are still populated:
 - `EvaluationTime`—The time it took for the policy to be evaluated.
 - `PolicyOutcome`—Set to `NoAction`.
 - `PolicyId`—Set to `null`.

Recommended Usage of Event Objects

Real-Time Event Monitoring objects have three primary uses: streaming data, storing data, and enforcing policies on data. But these uses don't apply to all objects. Here's guidance on which objects are available for each use case. For details, see [Stream and Store Event Data](#).

Streaming	Storage	Policy
ApiEventStream	ApiEvent	ApiEvent
LightningUriEventStream	LightningUriEvent	n/a
ListViewEventStream	ListViewEvent	ListViewEvent
LoginAsEventStream	LoginAsEvent	n/a
LoginEventStream	LoginEvent	LoginEvent
LogoutEventStream	LogoutEvent	n/a
ReportEventStream	ReportEvent	ReportEvent
UriEventStream	UriEvent	n/a

 **Note:** Real-Time Event Monitoring Platform Events aren't a system of record for user activity. They're a source of truth but event notifications aren't always available or guaranteed. For more reliable data storage, use [Real-Time Event Monitoring Storage Events](#) on page 1068.

Enable Access to Real-Time Event Monitoring

You can set user access to Real-Time Event Monitoring through profiles and permission sets.

- Do one of the following.
 - From Setup, in the Quick Find box, enter *Permission Sets*, and then select **Permission Sets**.
 - From Setup, in the Quick Find box, enter *Profiles*, and then select **Profiles**.
- Select a permission set or profile.
- Depending on whether you're using permission sets or profiles, do one of the following.
 - In permission sets or the enhanced profile user interface, select a permission. In the Find Settings dialog box, enter *View Real-Time Event Monitoring Data*. Click **Edit**, select the option, and click **Save**. Repeat these steps for the Customize Application permission.
 - In the original profile user interface, select a profile name, and then click **Edit**. Select **View Real-Time Event Monitoring Data**, **View All Data**, and **Customize Application** if you plan to create transaction security policies. Click **Save**.

In addition to enabling Real-Time Event Monitoring, set user permissions to Real-Time Event objects. Real-Time Event Monitoring objects sometimes contain sensitive data.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

USER PERMISSIONS

To view events:

- View Real-Time Event Monitoring Data

To view transaction security policies:

- View All Data

To create, edit, and manage transaction security policies:

- Customize Application

Stream and Store Event Data

Explore how you can use the objects in Real-Time Event Monitoring to stream and store event data.

[Manage Real-Time Event Monitoring Events](#)

Manage streaming and storage settings for Real-Time Event Monitoring events declaratively with the Event Manager. You can also manage settings programmatically with the Metadata API. Real-Time Event Monitoring helps you monitor and detect standard events in Salesforce in near real-time. You can store the event data for auditing or reporting purposes. You can create transaction security policies using Condition Builder—a point-and-click tool—or Apex code.

[Real-Time Event Monitoring Data Streaming](#)

Use Real-Time Event Monitoring to subscribe to standard events published by Salesforce to monitor activity in your org. You can subscribe to this data from an external data system of your choice using a streaming API client.

[Real-Time Event Monitoring Data Storage](#)

With Real-Time Event Monitoring, you can store and query event data in Salesforce objects. Many of the storage events are Salesforce big objects, which are ideal for storing large volumes of data for up to six months. A big object stores the data natively in Salesforce so you can access it for reporting and other uses. Some storage events, such as for Threat Detection, are standard Salesforce objects.

[Use Async SOQL with Real-Time Event Monitoring](#)

Here are some examples of using Async SOQL with real-time events.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Manage Real-Time Event Monitoring Events

Manage streaming and storage settings for Real-Time Event Monitoring events declaratively with the Event Manager. You can also manage settings programmatically with the Metadata API. Real-Time Event Monitoring helps you monitor and detect standard events in Salesforce in near real-time. You can store the event data for auditing or reporting purposes. You can create transaction security policies using Condition Builder—a point-and-click tool—or Apex code.

 **Important:** Viewing Real-Time Event Monitoring events requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions. You don't need this add-on to view streaming logout events.

 **Note:** Real-Time Event Monitoring objects sometimes contain sensitive data. Assign object permissions to Real-Time Events accordingly in profiles or permission sets.

1. From Setup, in the Quick Find box, enter *Events*, then select **Event Manager**.
2. Next to the event you want to enable or disable streaming for, click the dropdown menu.
3. Select whether you want to enable or disable streaming or storing on the event.

SEE ALSO:

[Real-Time Event Monitoring](#)

[Stream and Store Event Data](#)

[Metadata API Developer Guide: RealTimeEventSettings](#)

USER PERMISSIONS

To update events in Event Manager:

- **Customize Application AND View Setup**

Real-Time Event Monitoring Data Streaming

Use Real-Time Event Monitoring to subscribe to standard events published by Salesforce to monitor activity in your org. You can subscribe to this data from an external data system of your choice using a streaming API client.

Data is streamed using a publish-subscribe model. Salesforce publishes streaming data to an event subscription channel, and your app subscribes, or listens, to the event channel to get the data close to real time. Streaming events are retained for up to three days. Real-Time Event Monitoring's streaming events don't count against your Platform Events delivery allocation. Some system protection limits apply. For example, Salesforce delivers a maximum of 50 million real-time events per day.

 **Tip:** To more efficiently obtain and process event data from three days ago or less, we recommend querying events from big objects instead of subscribing to past events in a stream.

Here are some examples.

Event Object	Use Case	Considerations
ApiEventStream	Detect when a user queries sensitive data, such as patent records.	Object is available only in Real-Time Event Monitoring.
ApiAnomalyEvent	Track anomalies in how users make API calls.	Object is available only in Real-Time Event Monitoring.
BulkApiResultEvent	Track when a user downloads the results of a Bulk API or Bulk API 2.0 request.	Object is available only in Real-Time Event Monitoring.
ConcurLongRunApexErrEvent	Detect errors that occur when an org exceeds the concurrent long-running Apex limit.	Object is available only in Real-Time Event Monitoring.
CredentialStuffingEvent	Track when a user successfully logs into Salesforce during an identified credential stuffing attack. Credential stuffing refers to large-scale automated login requests using stolen user credentials.	Object is available only in Real-Time Event Monitoring.
FileEvent	Detects file-related events, such as when a user downloads a file.	Object is available only in Real-Time Event Monitoring.
LightningUriEventStream	Detect when a user creates, accesses, updates, or deletes a record containing sensitive data in Lightning Experience.	Object is available only in Real-Time Event Monitoring.
ListViewEventStream	Detect when a user accesses, updates, or exports list view data using Salesforce Classic, Lightning Experience, or the API.	Object is available only in Real-Time Event Monitoring.
LoginAsEventStream	Detect when a Salesforce admin logs in as another user and track the admin's activities.	Object is available only in Real-Time Event Monitoring.
LoginEventStream	Detect when a user tries to log in under certain conditions—for example, from an unsupported browser or from an IP address that is outside of your corporate range.	Object is available only in Real-Time Event Monitoring.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Event Object	Use Case	Considerations
LogoutEventStream	Detect when a user logs out of Salesforce by clicking Log Out in the Salesforce UI.	Object is available to all customers.
MobileEmailEvent	Track your users' email activity in a Salesforce mobile app.	Object is available only in Real-Time Event Monitoring and Enhanced Mobile App Security.
MobileEnforcedPolicyEvent	Track enforcement of Enhanced Mobile Security policy events on a Salesforce mobile app.	Object is available only in Real-Time Event Monitoring and Enhanced Mobile App Security.
MobileScreenshotEvent	Track your users' screenshots in a Salesforce mobile app.	Object is available only in Real-Time Event Monitoring and Enhanced Mobile App Security.
MobileTelephonyEvent	Track your users' phone calls and text messages in a Salesforce mobile app.	Object is available only in Real-Time Event Monitoring and Enhanced Mobile App Security.
PermissionSetEvent	Detect permission assignment changes in permission sets and permission set groups.	Object is available only in Real-Time Event Monitoring.
ReportAnomalyEvent	Track anomalies in how users run or export reports.	Object is available only in Real-Time Event Monitoring.
ReportEventStream	Detect when a user creates, runs, updates, or exports a report that contains sensitive data.	Object is available only in Real-Time Event Monitoring.
SessionHijackingEvent	Track when unauthorized users gain ownership of a Salesforce user's session with a stolen session identifier.	Object is available only in Real-Time Event Monitoring.
UriEventStream	Detect when a user creates, accesses, updates, or deletes a record containing sensitive data in Salesforce Classic.	Object is available only in Real-Time Event Monitoring

For more information about building apps that listen to streaming data channels, see the [Streaming API Developer Guide](#).

For a quick start about subscribing to streaming events using the EMP Connector open-source tool, see the [Example: Subscribe to and Replay Events Using a Java Client \(EMP Connector\)](#) in the *Platform Events Developer Guide*.

For reference documentation of the standard platform events and the corresponding big objects, see [Real-Time Event Monitoring Objects](#) in the *Platform Events Developer Guide*.

Real-Time Event Monitoring Data Storage

With Real-Time Event Monitoring, you can store and query event data in Salesforce objects. Many of the storage events are Salesforce big objects, which are ideal for storing large volumes of data for up to six months. A big object stores the data natively in Salesforce so you can access it for reporting and other uses. Some storage events, such as for Threat Detection, are standard Salesforce objects.

Using SOQL with Storage Events

Standard and Async SOQL queries are supported for both types of storage events: big objects and standard objects.

Standard SOQL

Standard objects, such as the Threat Detection storage events, support SOQL queries on all their fields. But big objects support SOQL queries on only two fields: `EventDate` or `EventIdentifier`. You can query big objects using a subset of standard SOQL commands filtering by `EventDate` alone, or `EventDate` and `EventIdentifier` together.

The exception is `ReportEvent`, where you can filter on three fields: `EventDate`, `EventIdentifier`, and `UserId` (Beta). Valid filters for `ReportEvent` queries are: If you filter on `EventIdentifier` alone, or `UserId` with `EventIdentifier`, your query fails. You can only do a range query on the first index when you're searching on `UserId` alone.

- `UserId` alone
- `EventDate` alone
- `UserId` with `EventDate`
- `EventDate` with `EventIdentifier`

 **Note:** As a beta feature, the `UserId` filter in `ReportEvent` is a preview and isn't part of the "Services" under your Main Services Agreement with Salesforce. Use this feature at your sole discretion, and make your purchase decisions only on the basis of generally available products and features. Salesforce doesn't guarantee general availability of this feature within any particular time frame or at all, and we can discontinue it at any time. This feature is for evaluation purposes only, not for production use. It's offered as is and isn't supported, and Salesforce has no liability for any harm or damage arising out of or in connection with it. All restrictions, Salesforce reservation of rights, obligations concerning the Services, and terms for related Non-Salesforce Applications and Content apply equally to your use of this feature.

Async SOQL

Async SOQL is a way to run SOQL queries when you must filter on big object fields other than `EventDate` and `EventId`. Async SOQL schedules and runs queries asynchronously in the background, so it can run queries that normally time out with regular SOQL.

With Async SOQL, you can run multiple queries in the background while monitoring their completion status. Set up your queries and come back a few hours later to a dataset to work with. Async SOQL is the most efficient way to process the large amount of data in a storage event, especially for big objects. For more information, see [Use Async SOQL with Real-Time Event Monitoring](#) and [Async SOQL in the Big Objects Implementation Guide](#).

Storage Events

Here are the Real-Time Event Monitoring storage events.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Unlimited**, and **Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Event Object	Standard or Big Object?	Use Case	Considerations
ApiEvent	Big Object	Store data about all API activity that occurred for particular objects during a fiscal year.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 6 months.
ApiAnomalyEventStore	Standard Object	Store data about anomalies in how users make API calls.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 6 months.
BulkApiResultEventStore	Big Object	Store large amount of data about Bulk API activity that occurred for particular objects during a fiscal year.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 6 months.
CredentialStuffingEventStore	Standard Object	Store data about successful user logins during an identified credential stuffing attack. Credential stuffing refers to large-scale automated login requests using stolen user credentials.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 6 months.
FileEventStore	Big Object	Stores file-related event data, such as when a user downloads a file.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 6 months.
IdentityVerificationEvent	Big Object	Store data about user identity verification events in your org.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 10 years.
IdentityProviderEventStore	Big Object	Store data about problematic and successful authentication requests in the Identity Provider Event Log.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 6 months.
LightningUriEvent	Big Object	Store data about when entities are created, accessed, updated, or deleted in Lightning Experience.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 6 months.
ListViewEvent	Big Object	Store data about when users interact with a list of records, such as contacts, accounts, or custom objects.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 6 months.
LoginAsEvent	Big Object	Store data about when Salesforce admins log in as another user.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 6 months.
LoginEvent	Big Object	Store data about how many users tried to log in from an unknown IP address or location and who was blocked from successfully logging in.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 10 years.
LogoutEvent	Big Object	Store data about users who logged out successfully.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 6 months.

Event Object	Standard or Big Object?	Use Case	Considerations
PermissionSetEventStore	Big Object	Store data about permission assignment changes in permission sets and permission set groups.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 6 months.
ReportAnomalyEventStore	Standard Object	Store data about anomalies in how users run or export reports.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 6 months.
ReportEvent	Big Object	Store data about how many times a sensitive report was downloaded or viewed and by whom.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 6 months.
SessionHijackingEventStore	Standard Object	Store data about when unauthorized users gain ownership of a Salesforce user's session with a stolen session identifier.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 6 months.
UriEvent	Big Object	Store data about when entities are created, accessed, updated, or deleted in Salesforce Classic.	Object is available only in Real-Time Event Monitoring. Data is stored for up to 6 months.

 **Note:** In Developer Edition orgs, data for all events is stored for only one day.

Use Async SOQL with Real-Time Event Monitoring

Here are some examples of using Async SOQL with real-time events.

 **Note:** Async SOQL is scheduled for retirement in all Salesforce orgs as of Summer '23.

Let's say you've created a custom object called Patent__c that contains sensitive patent information. You want to know when users query this object using any API. Use the following Async SOQL query on the ApiEvent object to determine when Patent__c was last accessed, who accessed it, and what part of it was accessed. The WHERE clause uses the `QueriedEntities` field to narrow the results to just API queries of the Patent__c object.

Example URI

```
https://yourInstance.salesforce.com/services/data/v48.0/async-queries/
```

Example POST request body

```
{
  "query": "SELECT EventDate, EventIdentifier, QueriedEntities, SourceIp, Username,
  UserAgent FROM ApiEvent
  WHERE QueriedEntities LIKE '%Patent__c%'",
  "targetObject": "ApiTarget__c",
  "targetFieldMap": {
    "EventDate": "EventDate__c",
    "EventIdentifier": "EventIdentifier__c",
    "QueriedEntities": "QueriedEntities__c",
    "SourceIp": "IPAddress__c",
    "Username": "User__c",
    "UserAgent": "UserAgent__c"
  }
}
```

```
}
}
```

Example POST response body

```
{
  "jobId" : "08PB00000066JrfMAM",
  "message" : "",
  "operation" : "INSERT",
  "query" : "SELECT EventDate, EventIdentifier, QueriedEntities, SourceIp, Username,
UserAgent FROM ApiEvent
          WHERE QueriedEntities LIKE &#39;%Patent__c&#39;",
  "status" : "Complete",
  "targetExternalIdField" : "",
  "targetFieldMap" : {
    "EventDate" : "EventDate__c",
    "SourceIp" : "IPAddress__c",
    "EventIdentifier" : "EventIdentifier__c",
    "QueriedEntities" : "QueriedEntities__c",
    "Username" : "User__c",
    "UserAgent" : "UserAgent__c"
  },
  "targetObject" : "ApiTarget__c",
  "targetValueMap" : { }
}
```

 **Note:** All number fields returned from a SOQL query of archived objects are in standard notation, not scientific notation, as in the number fields in the entity history of standard objects.

If you ask this question on a repeated basis for audit purposes, you can automate the query using a cURL script.

```
curl -H "Content-Type: application/json" -X POST -d
'{"query": "SELECT EventDate, EventIdentifier, QueriedEntities, SourceIp, Username, UserAgent
FROM ApiEvent WHERE QueriedEntities LIKE '%Patent__c'",
  "targetObject": "ApiTarget__c",
  "targetFieldMap": {"EventDate": "EventDate__c", "EventIdentifier":
"EventIdentifier__c", "QueriedEntities": "QueriedEntities__c", "SourceIp":
"IPAddress__c", "Username": "User__c", "UserAgent": "UserAgent__c"}}'
https://yourInstance.salesforce.com/services/data/v48.0/async-queries/" -H
"Authorization: Bearer 00D30000000V88A!ARYAQZOCeABY29c3dNxRVtv433znH15gLWhLOUv7DVu.
uAGFhW9WMtGXCul6q.4xVQymfh4Cjxw4APbazT8bnIfx1RvUjDg"
```

Another event monitoring use case is to identify all users who accessed a sensitive field, such as Social Security Number or Email. For example, you can use the following Async SOQL query to determine the users who saw social security numbers.

Example URI

```
https://yourInstance.salesforce.com/services/data/v48.0/async-queries/
```

Example POST request body

```
{
  "query": "SELECT Query, Username, EventDate, SourceIp FROM ApiEvent
          WHERE Query LIKE '%SSN__c'",
  "targetObject": "QueryEvents__c",
  "targetFieldMap": {
```

```

    "Query": "QueryString__c",
    "Username": "User__c",
    "EventDate": "EventDate__c",
    "SourceIp" : "IPAddress__c"
  }
}

```

Example POST response body

```

{
  "jobId": "08PB000000001RS",
  "message": "",
  "query": "SELECT Query, Username, EventDate, SourceIp FROM ApiEvent
          WHERE Query LIKE &#39;%SSN__c&#39;",
  "status": "Complete",
  "targetFieldMap": {"Query": "QueryString__c", "Username": "User__c",
                    "EventDate": "EventDate__c", "SourceIp" : "IPAddress__c"
                    },
  "targetObject": "QueryEvents__c"
}

```

SEE ALSO:

[Big Objects Implementation Guide: Async SOQL](#)

Create Logout Event Triggers

If the `LogoutEventStream` object is available to your org, you can create Apex triggers that respond to security logout events from your org's UI.

When `LogoutEventStream` is enabled, Salesforce publishes logout events when users log out from the UI. You can add an Apex trigger to subscribe to those events. You can then implement custom logic during logout. For example, you can revoke all refresh tokens for a user at logout.

Timeouts don't cause a `LogoutEventStream` object to be published. An exception is when a user is automatically logged out of the org after their session times out because the org has the **Force logout on session timeout** setting enabled. In this case, a logout event is recorded. However, if users close their browser during a session, regardless of whether the **Force logout on session timeout** setting is enabled, a logout event isn't recorded.

1. From Setup, enter *Event Manager* in the Quick Find box, then select **Event Manager**.
2. Next to Logout Event, click the dropdown, and select **Enable Streaming**.
3. Create Apex triggers that subscribe to logout events.



Example: In this example, the subscriber inserts a custom logout event record during logout.

```

trigger LogoutEventTrigger on LogoutEventStream (after insert) {
  LogoutEventStream event = Trigger.new[0];
  LogoutEvent__c record = new LogoutEvent__c();
  record.EventIdentifier__c = event.EventIdentifier;
  record.UserId__c = event.UserId;
  record.Username__c = event.Username;
  record.EventDate__c = event.EventDate;
}

```

EDITIONS

Available in: **All Editions**

```

record.RelatedEventIdentifier__c = event.RelatedEventIdentifier;
record.SessionKey__c = event.SessionKey;
record.LoginKey__c = event.LoginKey;
insert(record);
}

```

How Chunking Works with ReportEvent and ListViewEvent

Chunking occurs when a report or list view execution returns many records and Salesforce splits the returned data into chunks.

 **Tip:** This topic applies to ReportEvent, ReportEventStream, ListViewEvent, and ListViewEventStream. However, for readability, we refer to just ReportEvent and ListViewEvent.

When Salesforce chunks a ReportEvent or ListViewEvent (and their streaming equivalents), it breaks it into multiple events in which most field values are repeated. The exceptions are the `Records`, `Sequence`, and `EventIdentifier` fields. You view all the data from a chunked result by correlating these fields with the `ExecutionIdentifier` field, which is unique across the chunks.

 **Important:** When a report executes, we provide the first 1000 events with data in the `Records` field. Use the `ReportId` field to view the full report.

Let's describe in more detail the fields of ReportEvent and ListViewEvent (and their storage equivalents) that you use to link together the chunks.

- `Records`—A JSON string that represents the report or list view data. If Salesforce has chunked the data into multiple events, each event's `Records` field contains different data.
- `Sequence`—An incremental sequence number that indicates the order of multiple events that result from chunking, starting with 1. For example, if Salesforce breaks up an event into five chunks, the first chunk's `Sequence` field is 1, the second is 2, and so on up to 5.
- `ExecutionIdentifier`—A unique identifier for a particular report or list view execution. This identifier differentiates the report or list execution from other executions. If chunking has occurred, this field value is identical across the chunks, and you can use it to link the chunks together to provide a complete data picture.
- `EventIdentifier`—A unique identifier for each event, including chunked events.

To view all the data chunks from a single report or list view execution, use the `Sequence`, `Records`, and `ExecutionIdentifier` fields in combination.

For example, let's say a report execution returns 10K rows. Salesforce splits this data into three chunks based on the size of the records, and then creates three separate ReportEvent events. This table shows an example of the field values in the three events; the fields not shown in the table (except `EventIdentifier`) have identical values across the three events.

ExecutionIdentifier	Sequence	Records
a50a4025-84f2-425d-8af9-2c780869f3b5	1	{"totalSize":3000, "rows":[{"datacells":["005B0000001vURv",.....]}}}
a50a4025-84f2-425d-8af9-2c780869f3b5	2	{"totalSize":3000, "rows":[{"datacells":["005B000000fewai",.....]}}}

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Unlimited**, and **Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

ExecutionIdentifier	Sequence	Records
a50a4025-84f2-425d-8af9-2c780869f3b5	3	{"totalSize":4000, "rows":[{"datacells":["005B0000001vURv",.....]}]}

This sample SOQL query returns data similar to the preceding table.

```
SELECT ExecutionIdentifier, Sequence, Records FROM ReportEvent
```

How Transaction Security Works With Chunking

If a chunked event triggers a transaction security policy, Salesforce executes the policy on only the first chunk. The `PolicyId`, `PolicyOutcome`, and `EvaluationTime` field values are repeated in all the chunked events. These tables show different policy actions and execution outcomes and their resulting events, some of which are chunked.

This event results from a triggered policy that had a block action.

ExecutionIdentifier (value shortened for readability)	Sequence	Records	PolicyId (value shortened for readability)	PolicyOutcome	EvaluationTime
a50a4...9-2c780869f3b5	0	{"totalSize":0, "rows":{}}	0Nlxx...GA2	Block	30

These events result from a triggered policy that has a multi-factor authentication (MFA) action. The first three rows show the multi-factor authentication in process, and the last three rows show the chunked events.

 **Note:** Multi-factor authentication was previously called two-factor authentication. Some MFA-related values reference "TwoFa".

ExecutionIdentifier (value shortened for readability)	Sequence	Records	PolicyId (value shortened for readability)	PolicyOutcome	EvaluationTime
a50a4...9-2c780869f3b5	0	{"totalSize":0, "rows":{}}	0Nlxx...GA2	TwoFaInitiated	30
				TwoFaInProgress	
				TwoFaSucceed	
43805...e-5914976709c4	2	{"totalSize":3000, "rows":[{"datacells":["005B000000feval",.....]}]}	0Nlxx...GA2	TwoFaNoAction	24
43805...e-5914976709c4	3	{"totalSize":4000, "rows":[{"datacells":["005B0000001vURv",.....]}]}	0Nlxx...GA2	TwoFaNoAction	24
43805...e-5914976709c4	1	{"totalSize":3000, "rows":[{"datacells":["005B0000001vURv",.....]}]}	0Nlxx...GA2	TwoFaNoAction	24

These events result from a policy that has a block action but the event didn't meet the condition criteria. As a result, the `PolicyOutcome` field is `NoAction`.

ExecutionIdentifier (value shortened for readability)	Sequence	Records	PolicyId (value shortened for readability)	PolicyOutcome	ElapsedTime
a50a4...9-2c780869f3b5	1	{"totalSize":3000, "rows":{"datacells":{"005B0000001vURV",_____}}}	0Nlxx...GA2	NoAction	24
a50a4...9-2c780869f3b5	2	{"totalSize":3000, "rows":{"datacells":{"005B000000fewai",_____}}}	0Nlxx...GA2	NoAction	24
a50a4...9-2c780869f3b5	3	{"totalSize":4000, "rows":{"datacells":{"005B0000001vURV",_____}}}	0Nlxx...GA2	NoAction	24

These events result from a policy that has a multi-factor authentication action but the policy wasn't triggered and so the action didn't occur. The policy didn't trigger because the user already had a high assurance session level.

ExecutionIdentifier (value shortened for readability)	Sequence	Records	PolicyId (value shortened for readability)	PolicyOutcome	ElapsedTime
a50a4...9-2c780869f3b5	1	{"totalSize":3000, "rows":{"datacells":{"005B0000001vURV",_____}}}	0Nlxx...GA2	TwoFaNoAction	24
a50a4...9-2c780869f3b5	2	{"totalSize":3000, "rows":{"datacells":{"005B000000fewai",_____}}}	0Nlxx...GA2	TwoFaNoAction	24
a50a4...9-2c780869f3b5	3	{"totalSize":4000, "rows":{"datacells":{"005B0000001vURV",_____}}}	0Nlxx...GA2	TwoFaNoAction	24

Enhanced Transaction Security

Enhanced Transaction Security is a framework that intercepts real-time events and applies appropriate actions to monitor and control user activity. Each transaction security policy has conditions that evaluate events and the real-time actions that are triggered after those conditions are met. The actions are Block, Multi-Factor Authentication, and Notifications. Before you build your policies, understand the available event types, policy conditions, and common use cases. Enhanced Transaction Security is included in Real-Time Event Monitoring.

Condition Builder vs. Apex

Condition Builder is a Setup feature that allows you to build policies with clicks, not code. Policies monitor events, which are categories of user activity built on objects in the SOAP, REST, and Bulk APIs. When you build your policy using Condition Builder, you choose which fields on these objects you want to monitor for customer activity. Because your policy's actions are conditional to the fields that users interact with, these fields are called *conditions*. When you create a policy, you choose the conditions you want your policy to monitor and the action the policy takes when the conditions are met. The conditions available in Condition Builder are a subset of all the event objects fields and vary based on the objects.

If you create an Apex-based policy, you can use any of the event object's fields. For example, Records isn't available as a Condition Builder condition for the ReportEvent event object. But you can use the `ReportEvent.Records` field in an Apex class that implements the `TxnSecurity.EventCondition` interface. Visit the API Object Reference to view event object fields.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Conditions at a Glance

Event Object	Conditions Available in Condition Builder	Actions
ApiEvent	API Type, API Version, Application, Client, Elapsed Time, Operation, Platform, Queried Entities, Query, Rows Processed, Session Level, Source IP, User Agent, User ID, Username	Block, Notifications
ApiAnomalyEventStore	User, Username, SourceIp, Score, QueriedEntities, Operation, RowsProcessed, UserAgent	Notifications
BulkApiResultEventStore	Query, SessionLevel, SourceIp, UserId, Username	Block, Notifications
CredentialStuffingEventStore	AcceptLanguage, LoginUrl, Score, SourceIp, UserAgent, UserId, Username	Notifications
FileEventStore	Can Download PDF, Content Size, Content Download ID, Content Version ID, Evaluation Time, File Action, File Name, File Source, File Type, Is Latest Version, Policy Outcome, Process Duration, Session Level, Source IP, Transaction Security Policy ID, User ID, Username, Version Number	Block, Notifications
ListViewEvent	Application Name, Developer Name, Event Source, List View ID, Name, Name of Columns, Number of Columns, Order By, Owner ID, Queried Entities, Rows Processed, Scope, Session Level, Source IP, User ID, Username	Block, Notifications, Multi-Factor Authentication (for UI logins) Multi-factor authentication isn't supported for list views in Lightning pages, so the action is upgraded to Block.
LoginEvent	API Type, API Version, Application, Authentication Method Reference, Browser, Country, Login Subtype, Login Type, Login URL, Platform, Session Level, Source IP, TLS Protocol, User ID, User Type, Username	Block, Notifications, Multi-Factor Authentication (for UI logins)
PermissionSetEventStore	Event Source, Operation, Permission Type, User Count, User ID, Username	Block, Notifications
PermissionSetEventStore	Event Source, Operation, Permission Type, User Count, User ID, Username	Block, Notifications
ReportAnomalyEventStore	Report, Score, SourceIp, UserId, Username	Notifications
ReportEvent	Dashboard ID, Dashboard Name, Description, Event Source, Format, Is Scheduled, Name, Name of Columns, Number of Columns, Operation, Owner ID,	Block, Notifications, Multi-Factor Authentication (for UI logins)

Event Object	Conditions Available in Condition Builder	Actions
	Queried Entities, Report ID, Rows Processed, Scope, Session Level, Source IP, User ID, Username	
SessionHijackingEventStore	CurrentUserAgent, CurrentIp, CurrentPlatform, CurrentScreen, CurrentWindow, PreviousUserAgent, PreviousIp, PreviousPlatform, PreviousScreen, PreviousWindow, Score, SourceIp, UserId, Username	Notifications

[Types of Enhanced Transaction Security Policies](#)

You can create transaction security policies on these Real-Time Event Monitoring events.

[Enhanced Transaction Security Actions and Notifications](#)

When a real-time event triggers a transaction security policy, you can block a user or enforce multi-factor authentication (MFA). You can also optionally receive in-app or email notifications of the event.

[Build a Transaction Security Policy with Condition Builder](#)

Create a transaction security policy without writing a line of code. Condition Builder, available in Real-Time Event Monitoring, gives you a declarative way to create customized security policies to protect your data.

[Create an Enhanced Transaction Security Policy That Uses Apex](#)

Use Setup to create an enhanced transaction security policy that uses Apex. You can specify an existing Apex class or create an empty class that you then code. The Apex class must implement the `TxnSecurity.EventCondition` interface.

[Best Practices for Writing and Maintaining Enhanced Transaction Security Policies](#)

Transaction security policy management isn't always easy, especially when you have many policies. To make sure that your policies remain functional, write and maintain them using these best practices. Well-structured and tested policies keep your employees and customers connected, productive, and secure.

[Enhanced Transaction Security Metering](#)

Transaction Security uses resource metering to help prevent malicious or unintentional monopolization of shared, multi-tenant platform resources. Metering prevents transaction security policy evaluations from using too many resources and adversely affecting your Salesforce org.

[Exempt Users from Transaction Security Policies](#)

If you have transaction security policies that work well for most users, but not all, you can assign specific users the Exempt from Transaction Security user permission. Assign this permission only when transaction security policy metering regularly blocks business-critical actions. For example, assign it to users who make bulk or automated bulk API calls. You can assign this user permission to integration users or admins responsible for transaction security policies who you don't want to get blocked.

[Test and Troubleshoot Your New Enhanced Policy](#)

If your enhanced transaction security policy isn't behaving as you expect, check out these testing and troubleshooting tips to diagnose the problem.

Types of Enhanced Transaction Security Policies

You can create transaction security policies on these Real-Time Event Monitoring events.

[ApiEvent Policies](#)

API events monitor API transactions, such as SOQL queries and data exports.

[ApiAnomalyEventStore Policies](#)

API anomaly event policies monitor anomalies in how users make API calls.

[BulkApiResultEventStore Policies](#)

Bulk API Result Event policies detect when a user downloads the results of a Bulk API request.

[CredentialStuffingEventStore Policies](#)

Credential stuffing event policies monitor when a user successfully logs into Salesforce during an identified credential stuffing attack. Credential stuffing refers to large-scale automated login requests using stolen user credentials.

[FileEvent Policies](#)

File event policies detect file-related events, such as when a user downloads a file containing sensitive information.

[ListViewEvent Policies](#)

List View event policies monitor when data is viewed or downloaded from your list views using Salesforce Classic, Lightning Experience, or the API.

[LoginEvent Policies](#)

Login event policies track login activity and enforce your login requirements.

[PermissionSetEventStore Policies](#)

Permission set event policies monitor when users are assigned critical permissions in a permission set.

[ReportEvent Policies](#)

Report event policies monitor when data is viewed or downloaded from your reports.

[ReportAnomalyEventStore Policies](#)

Report anomaly event policies monitor anomalies in how users run or export reports.

[SessionHijackingEventStore Policies](#)

Session hijacking event policies monitor when unauthorized users gain ownership of a Salesforce user's session with a stolen session identifier.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Unlimited**, and **Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

ApiEvent Policies

API events monitor API transactions, such as SOQL queries and data exports.

Policy at a Glance

Object	Conditions Available in Condition Builder	Actions	Considerations
ApiEvent	API Type, API Version, Application, Client, Elapsed Time, Operation, Platform, Queried Entities, Query, Rows Processed, Session Level, Source IP, User Agent, User ID, Username	Block, Notifications	Multi-factor authentication isn't supported.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Unlimited**, and **Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

What You Can Do With It

You can monitor user behaviors taken through the API on a granular level. Create a policy that can:

- Block access to particular versions of the API from specific platforms
- Notify you when users run queries that return many rows

Considerations for ApiEvent Policies

- The supported SOAP, REST, Bulk API, and Bulk API 2.0 calls are `query()`, `query_more()`, and `query_all()`. Transaction Security supports only `query()`. API calls made from Visualforce (via an Apex controller) or XMLRPC aren't supported in ApiEvent and ApiEventStream.
- For Bulk API and Bulk API 2.0 queries, expect blank values for `LoginHistoryId`, `Client`, and `UserAgent` in ApiEvent. These queries are asynchronous and executed by a background job.

ApiAnomalyEventStore Policies

API anomaly event policies monitor anomalies in how users make API calls.

Policy at a Glance

Object	Conditions Available in Condition Builder	Actions
ApiAnomalyEventStore	User, Username, Sourcelp, Score, QueriedEntities, Operation, RowsProcessed, UserAgent	Notifications

What You Can Do With It

Create a policy that can:

- Send you an email when Salesforce detects that a user has made more API calls than usual.
- Generate an in-app notification when Salesforce detects an API anomaly event with a score greater than 0.5.

BulkApiResultEventStore Policies

Bulk API Result Event policies detect when a user downloads the results of a Bulk API request.

Policy at a Glance

Object	Conditions Available in Condition Builder	Actions
BulkApiResultEventStore	Query, SessionLevel, Sourcelp, UserId, Username	Block, Notifications

What You Can Do With It

Create a policy that can:

- Send you an email when Salesforce detects that a user has attempted to download the results of a Bulk API request

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Unlimited**, and **Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

CredentialStuffingEventStore Policies

Credential stuffing event policies monitor when a user successfully logs into Salesforce during an identified credential stuffing attack. Credential stuffing refers to large-scale automated login requests using stolen user credentials.

Policy at a Glance

Object	Conditions Available in Condition Builder	Actions
CredentialStuffingEventStore	AcceptLanguage, LoginUrl, Score, SourceIp, UserAgent, UserId, Username	Notifications

What You Can Do with It

Create a policy that can:

- Send you an email when Salesforce detects that a user from a specific IP address successfully logged into your org during a credential stuffing attack.
- Generate an in-app notification when Salesforce detects a login from a specific page, such as `login.salesforce.com` or `MyDomainName.my.salesforce.com`, during a credential stuffing attack.

FileEvent Policies

File event policies detect file-related events, such as when a user downloads a file containing sensitive information.

Policy at a Glance

Object	Conditions Available in Condition Builder	Actions
FileEventStore	Can Download PDF, Content Size, Content Download ID, Content Version ID, Evaluation Time, File Action, File Name, File Source, File Type, Is Latest Version, Policy Outcome, Process Duration, Session Level, Source IP, Transaction Security Policy ID, User ID, Username, Version Number	Block, Notifications

What You Can Do with It

Create a policy that can:

- Notify administrators when a user attempts to preview a specific file.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

- Block downloads for specific user IDs, version IDs, and document IDs.

ListViewEvent Policies

List View event policies monitor when data is viewed or downloaded from your list views using Salesforce Classic, Lightning Experience, or the API.

Policy at a Glance

Object	Conditions Available in Condition Builder	Actions
ListViewEvent	Application Name, Developer Name, Event Source, List View ID, Name, Name of Columns, Number of Columns, Order By, Owner ID, Queried Entities, Rows Processed, Scope, Session Level, Source IP, User ID, Username	Block, Notifications, Multi-Factor Authentication (for UI logins) Multi-factor authentication isn't supported for list views in Lightning pages, so the action is upgraded to Block.

What You Can Do With It

Create a policy that can:

- Block a user who tries to access a list view of sensitive patent data
- Notify you if a user exports more than 5,000 rows from a list view in your org

 **Note:** The values captured by transaction security policies are unique API names that can be retrieved by performing REST API Describe calls on the object. When creating a ListViewEvent policy, make sure that the values you want the conditions to check for are unique API names and not display labels. For example, a “Name of Column” condition checks for values that match the metadata information retrieved from a Describe call on the report, not the column headers displayed on the report. Refer to the [REST API Developer Guide](#) for more information.

LoginEvent Policies

Login event policies track login activity and enforce your login requirements.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Policy at a Glance

Object	Conditions Available in Condition Builder	Actions	Considerations
LoginEvent	API Type, API Version, Application, Authentication Method Reference, Browser, Country, Login Subtype, Login Type, Login URL, Platform, Session Level, Source IP, TLS Protocol, User ID, User Type, Username	Block, Notifications, Multi-Factor Authentication (for UI logins)	<ul style="list-style-type: none"> • UI logins with username and password, SAML single sign-on logins, and API-based logins (OAuth, REST, SOAP) are captured. • Multi-factor authentication isn't supported for Lightning Login (passwordless login) users or for API-based logins. For API-based logins, the action is upgraded to Block. • LoginEvent policies aren't triggered by invalid login attempts such as incorrect passwords.

What You Can Do With It

You can target specific login behaviors that reduce performance or pose a security risk. Create a policy that can:

- Block users who log in from certain locations
- Require multi-factor authentication for users logging in from unsupported browsers
- Monitor logins from specific applications

How Does LoginEvent Compare to Login Log Lines and Login History?

Feature	LoginEvent (Login Forensics)	Login Log Lines	Login History
Standard Object or File	LoginEvent	EventLogFile (Login event type)	LoginHistory
Data Duration Until Deleted	6 months	30 days	6 months
Access	API	API download, Event Monitoring Analytics app	Setup UI, API
Permissions	View Real-Time Event Monitoring Data	View Event Log Files	Manage Users
Extensibility	Yes, using the AdditionalInfo field	No	No
Availability	Included with Event Monitoring add-on or Real-Time Event Monitoring	Included with Event Monitoring add-on	Included with all orgs

PermissionSetEventStore Policies

Permission set event policies monitor when users are assigned critical permissions in a permission set.

Policy at a Glance

Object	Conditions Available in Condition Builder	Actions
PermissionSetEventStore	Event Source, Operation, Permission Type, User Count, User ID, Username	Block, Notifications

What You Can Do with It

Create a policy that can:

- Prevent users from being assigned the following permissions in a permission set:
 - Assign Permission Sets
 - Author Apex
 - Customize Application
 - Manage Encryption Keys
 - Manage Internal Users
 - Manage Password Policies
 - Manage Profiles and Permission Sets
 - Manage Roles
 - Manage Sharing
 - Manage Users
 - Modify All Data
 - Multi-Factor Authentication for User Interface Logins
 - Password Never Expires
 - Reset User Passwords and Unlock Users
 - View All Data

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Unlimited**, and **Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

ReportEvent Policies

Report event policies monitor when data is viewed or downloaded from your reports.

Policy at a Glance

Object	Conditions Available in Condition Builder	Actions	Considerations
ReportEvent	Dashboard ID, Dashboard Name, Description, Event Source, Format, Is Scheduled, Name, Name of Columns, Number of Columns, Operation, Owner ID, Queried Entities, Report ID, Rows Processed, Scope, Session Level, Source IP, User ID, Username	Block, Notifications, Multi-Factor Authentication (for UI logins)	<p>Multi-factor authentication (MFA) policies apply to the following UI-based report actions:</p> <ul style="list-style-type: none"> Printable View Report Export Report Run (in Salesforce Classic only) <p>Multi-factor authentication isn't supported for reports in Lightning pages, so the action is upgraded to Block.</p>

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Unlimited**, and **Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

What You Can Do with It

Create a policy that can:

- Require multi-factor authentication for all users accessing or downloading reports over a specific size. For maximum coverage, write a policy that notifies you and blocks access to reports that process more than a certain number of rows.
- Block downloads for specific user IDs, report IDs, and dashboard IDs.

 **Note:** The values captured by transaction security policies are unique API names, which can be retrieved by performing REST API Describe calls on the object. When creating a ReportEvent policy, make sure that the values you want the conditions to check for are unique API names, not display labels. For example, a "Name of Column" condition checks for values that match the metadata information retrieved from a Describe call on the report, not the column headers displayed on the report. Refer to the [Salesforce Report and Dashboard REST API Developer Guide](#) for more information.

ReportAnomalyEventStore Policies

Report anomaly event policies monitor anomalies in how users run or export reports.

Policy at a Glance

Object	Conditions Available in Condition Builder	Actions
ReportAnomalyEventStore	Report, Score, Sourcelp, UserId, Username	Notifications

What You Can Do with It

Create a policy that can:

- Send you an email when Salesforce detects that a user has exported more records than usual from a report on Leads.
- Generate an in-app notification when Salesforce detects a report anomaly event with a score greater than 90.

SessionHijackingEventStore Policies

Session hijacking event policies monitor when unauthorized users gain ownership of a Salesforce user's session with a stolen session identifier.

Policy at a Glance

Object	Conditions Available in Condition Builder	Actions
SessionHijackingEventStore	CurrentUserAgent, CurrentIp, CurrentPlatform, CurrentScreen, CurrentWindow, PreviousUserAgent, PreviousIp, PreviousPlatform, PreviousScreen, PreviousWindow, Score, Sourcelp, UserId, Username	Notifications

What You Can Do with It

Create a policy that can:

- Generate an in-app notification when Salesforce detects a session hijacking attack on your org with a score greater than 10.
- Send you an email when Salesforce detects a session hijacking attack from a specific IP address.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

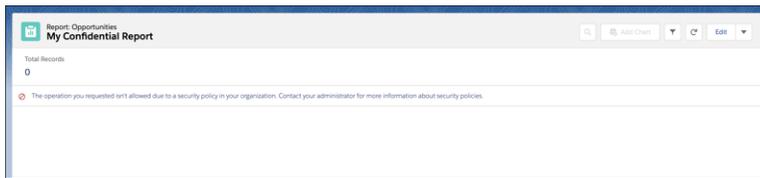
Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Enhanced Transaction Security Actions and Notifications

When a real-time event triggers a transaction security policy, you can block a user or enforce multi-factor authentication (MFA). You can also optionally receive in-app or email notifications of the event.

Block

Don't let the user complete the request. For example, if a ReportEvent policy with a block action triggers during a report view, the user sees a message explaining the action. You can also customize the block message when you create your policy. Each custom message can be up to 1000 characters, and you can only customize messages for ApiEvent, ListViewEvent, and ReportEvent policies. Custom block messages aren't translated.



Multi-Factor Authentication

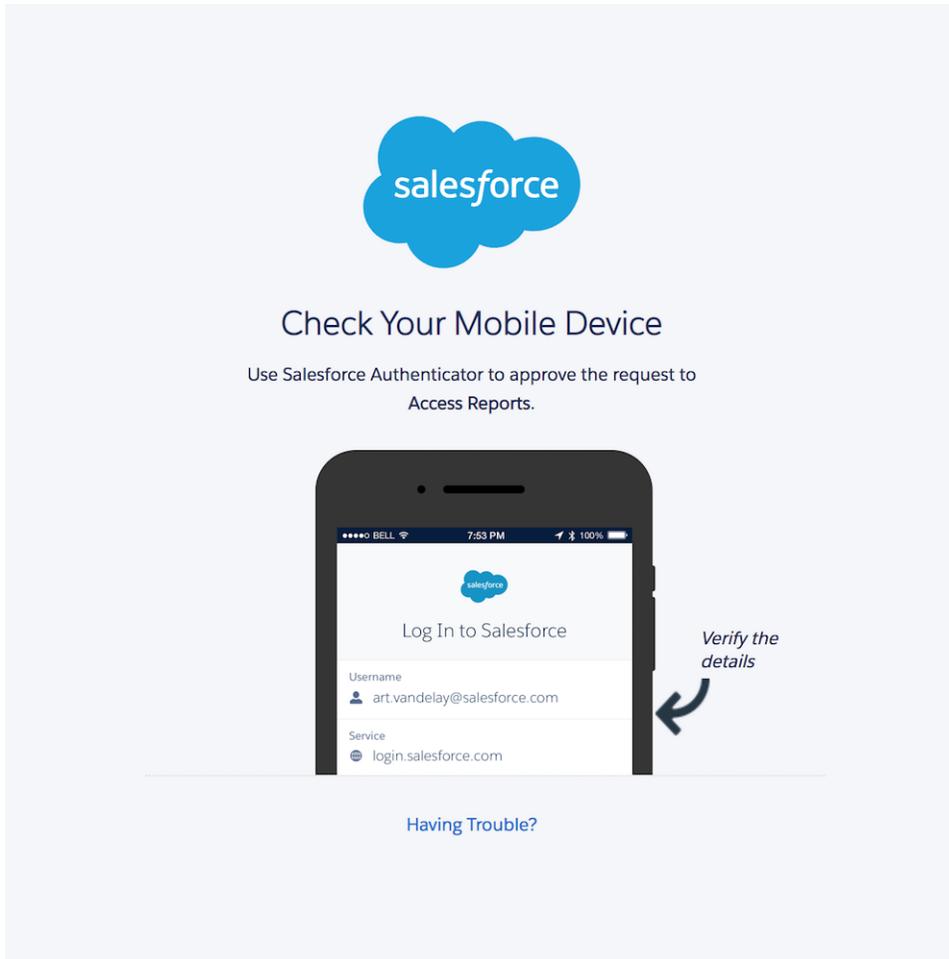
Prompt the user to confirm their identity with an additional verification method, such as the Salesforce Authenticator app, when they log in. In situations where you can't use multi-factor authentication (for instance, during an API query), this action changes to a block action.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Unlimited**, and **Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.



Email Notifications

You can send two kinds of email notifications when a policy is triggered: default email messages and custom email messages. Both use the subject Transaction Security Alert.

Default email notifications contain the policy that was triggered, the event or events that triggered it, the policy's ID, and related event fields. The times listed indicate when the policy was triggered in the recipient's locale and time zone. For example, a policy is triggered at 6:46 AM Eastern Standard Time. The administrator who receives the notification is in the Pacific Standard Time zone, so the time shows as PST. Here's an example.

```
From: Transaction Security <noreply@salesforce.com>
To: Admin@company.com
Sent: Wednesday, September 4, 2021, 10:00 AM
Subject: Transaction Security Alert
```

One of your transaction security policies was triggered.

```
Policy Name:
Restrict Views of the My Confidential Report
```

```
ID:
0NIRM00000000dV
```

```
Event responsible for triggering this policy:
ReportEvent associated with user lisa.johnson@company.com at 7/21/2021 06:46:11 AM PST
```

```
For more context about this event, refer to these event fields:
Org ID: 00DLA0000003YjP
User ID: 005IL000001ZqMb
```

Custom email notifications let you write your own email content and include event-specific field data of your choosing. To populate your message with field-level event data, use the lookup field. Salesforce recommends that you include only event information that the recipient is authorized to view. Custom email notifications aren't translated.

Notification ?

Email notification
 In-App notification

* Recipient
Jamal Jackson

* Email Notification Content ?

Default Email Content
 Custom Email Content

Someone tried to run a report that exceeds the 100 row limit. Use this event information to start your investigation.

- Organization ID - {{policy.OrganizationId}}
- User ID - {{event.UserId}}
- Event Name -

Choose your Event and Policy Fields

Select Fields...

- Policy Type
{{policy.Type}}
- Event Name
{{policy.EventName}}
- Transaction Security Policy ID
{{policy.Id}}
- Organization ID
{{policy.OrganizationId}}
- Name
{{policy.MasterLabel}}

* Name
Block 101 or more rows per r

Description

Status Enabled

In-App Notifications

In-app notifications list the policy that was triggered. Notifications aren't available in Classic. Here's an example.

Example:

```
Transaction Security Alert:
Policy Restrict Views of the My Confidential Report was triggered.
```

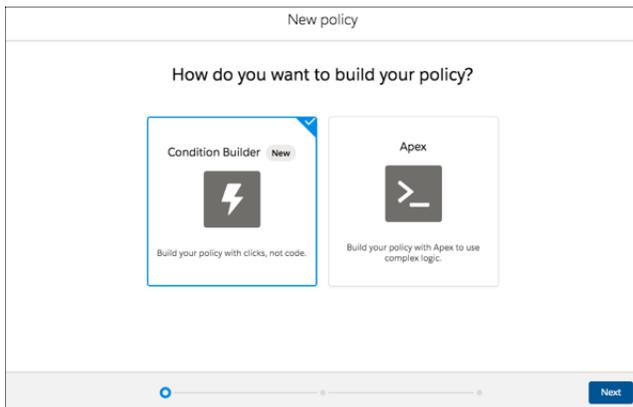
```
16 minutes ago
```

Build a Transaction Security Policy with Condition Builder

Create a transaction security policy without writing a line of code. Condition Builder, available in Real-Time Event Monitoring, gives you a declarative way to create customized security policies to protect your data.

You can create multiple policies for the same type of event, but we recommend that your policies and their actions don't overlap. If multiple policies with the same action for a given event execute when the event occurs, their order of execution is indeterminate.

1. From Setup, in the Quick Find box, enter *Transaction Security*, and then select **Transaction Security Policies**.
2. Click **New**, and then select **Condition Builder**.



3. Click **Next**.
4. Select an event that your policy is built on.
For example, if you want to track API calls in your org, select **API Event**. If you want to monitor when users view or export reports, select **Report Event**. See [Enhanced Transaction Security](#) for the full list of available events.
5. Select your condition logic. The logic applies to the conditions that you create in the next step.
You can specify whether all conditions must be met for the policy to trigger an action, or any condition.

Select **Custom Condition Logic Is Met** if you want to specify more complex logic. Use parentheses and logical operators (AND, OR, and NOT) to build the logical statements. Use numbers to represent each condition, such as 1 for the first condition and 2 for the second condition. For example, if you want the policy to trigger if the first condition and either the second or third conditions are met, enter `1 AND (2 OR 3)`.

6. Select your conditions.

Each condition has three parts:

- The event condition you want to monitor. The available conditions depend on the event you selected earlier. For example, you can monitor the number of rows that a user viewed in a report using the **Rows Processed** condition of Report Event. To monitor Salesforce entities that API calls query, use the **Queried Entities** condition of API Event. To monitor the IP addresses from which a user logged in, use the **Source IP** condition of Login Event.
- An operator, such as Greater Than or Starts With or Contains.
- A value that determines whether the condition is true or false. For example, if you specified the **Rows Processed** condition to monitor when users viewed more than 2,000 rows in a report, enter `2000`. If you specified the **Queried Entities** condition to monitor API calls against leads, enter `Lead`. If you specified the **Source IP** condition to monitor user logins from a specific IP address, enter the actual IP address, such as `192.0.2.255`.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

USER PERMISSIONS

To view events:

- View Real-Time Event Monitoring Data

To view transaction security policies:

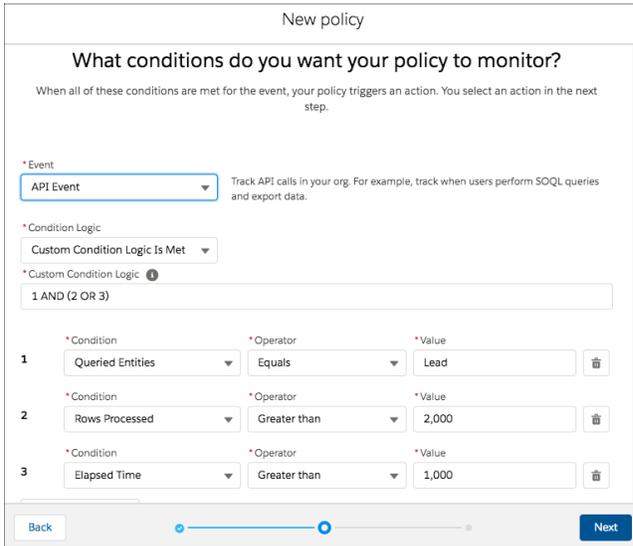
- View All Data

To create, edit, and manage transaction security policies:

- Customize Application

 **Tip:** Conditions map to fields of the event storage objects, such as `ApiEvent.RowsProcessed` or `LoginEvent.SourceIP`. See the [API documentation](#) for possible values and examples for each field that shows up as a condition in Condition Builder.

This example shows a policy that monitors API calls. The actions trigger if an API call queries the Lead object and either the number of rows processed is greater than 2000 or the request took longer than 1000 milliseconds to complete. See [Condition Builder Examples](#) for more examples.



The screenshot shows the 'New policy' configuration interface. The main heading is 'What conditions do you want your policy to monitor?'. Below this, there is a sub-heading: 'When all of these conditions are met for the event, your policy triggers an action. You select an action in the next step.'

The configuration includes the following elements:

- Event:** A dropdown menu set to 'API Event'. A tooltip below it reads: 'Track API calls in your org. For example, track when users perform SQL queries and export data.'
- Condition Logic:** A dropdown menu set to 'Custom Condition Logic Is Met'.
- Custom Condition Logic:** A text input field containing '1 AND (2 OR 3)'.
- Condition 1:** 'Queried Entities' (Condition) equals (Operator) 'Lead' (Value).
- Condition 2:** 'Rows Processed' (Condition) greater than (Operator) '2,000' (Value).
- Condition 3:** 'Elapsed Time' (Condition) greater than (Operator) '1,000' (Value).

At the bottom of the form, there are 'Back' and 'Next' buttons, along with a progress indicator.

7. Click **Next**.

8. Select what the policy does when triggered.

The actions available vary depending on the event type. For more information, see [Enhanced Transaction Security Actions and Notifications](#)

 **Note:** The multi-factor authentication action isn't available in the Salesforce mobile app, Lightning Experience, or via API for any events. Instead, the block action is used. For example, if a multi-factor authentication policy is triggered on a list view performed via the API, Salesforce blocks the API user.

9. Select who is notified and how.

10. Enter a name and description for your policy.

Your policy name can contain only underscores and alphanumeric characters and must be unique in your org. It must begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.

11. Optionally, enable the policy.

12. Click **Finish**.

Your policy is added to the list of available policies. When you enable Transaction Security policies for an event, some transaction run times related to that event can increase.

 **Important:** If you customize a Condition Builder policy with the API, you must include the Flow ID (for flow API), EventName, and Type of CustomConditionBuilderPolicy to save your policy.

[Condition Builder Examples](#)

Use these examples to help you convert your own real-world use cases into Condition Builder conditions.

Condition Builder Examples

Use these examples to help you convert your own real-world use cases into Condition Builder conditions.

Track Report Executions

Description of Example: Track when a user views or exports more than 2,000 rows from any report on the Lead object.

- **Event:** Report Event
- **Condition Logic:** All Conditions Are Met
- **Conditions:**
 - Rows Processed Greater Than 2,000
 - Queried Entities Contains Lead
- **Notes:** Use the **Contains** operator, rather than **Equals**, to also include reports that are based on multiple objects, one of which is Lead.

Description of Example: Track when a user views or exports a report that has a column that contains email addresses.

- **Event:** Report Event
- **Condition Logic:** All Conditions Are Met
- **Conditions:** Name of Columns Contains Email
- **Notes:** Use the **Contains** operator to include any of these column names: Email, Customer Email, or Email of Customer.

Track User Logins

Description of Example: Track when a user logs in from the IP address 12.34.56.78.

- **Event:** Login Event

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Unlimited**, and **Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

- **Condition Logic:** All Conditions Are Met
- **Conditions:** Source IP Equals 12.34.56.78
- **Notes:** Only the specific IP address 12.34.56.78 triggers the policy. If you want to track logins from any IP addresses that start with 12.34.56, use the condition Source IP Starts With 12.34.56.

The screenshot shows the configuration for a "Login Event". The "Event" dropdown is set to "Login Event". The "Condition Logic" dropdown is set to "All Conditions Are Met". There is one condition defined: "Source IP" with the operator "Equals" and the value "12.34.56.78". A "+ Add Condition" button is visible at the bottom left.

Description of Example: Track when a user logs in using a Chrome browser.

- **Event:** Login Event
- **Condition Logic:** All Conditions Are Met
- **Conditions:** Browser Contains Chrome
- **Notes:** You can also track logins from the Safari and Firefox browsers.

The screenshot shows a single condition configuration: "Browser" with the operator "Contains" and the value "Chrome". There is a trash icon to the right of the value field.

Track API Queries and Elapsed Time

Description of Example: Track when a user uses any API to query the Lead object and the request takes longer than 1,000 milliseconds.

- **Event:** API Event
- **Condition Logic:** All Conditions Are Met
- **Conditions:**
 - Queried Entities Contains Lead
 - Elapsed Time Greater Than 1000
- **Notes:** Use the **Contains** operator, rather than **Equals**, to also include queries on multiple objects, of which one is Lead.

The screenshot shows the configuration for an "API Event". The "Event" dropdown is set to "API Event". The "Condition Logic" dropdown is set to "All Conditions Are Met". There are two conditions defined, connected by an "AND" operator. The first condition is "Queried Entities" with the operator "Contains" and the value "Lead". The second condition is "Elapsed Time" with the operator "Greater than" and the value "1,000". There are trash icons to the right of both value fields. A "+ Add Condition" button is visible at the bottom left.

Track API Queries of Any List View

Description of Example: Track when a user uses any API to query any list view.

- **Event:** List View Event
- **Condition Logic:** All Conditions Are Met

- **Conditions:** Event Source Equals API
- **Notes:** To track when a user uses the UI to query a list view specify Classic or Lightning instead of API.

The screenshot shows the configuration for a List View Event. The event is set to "List View Event" with a description: "Track when users see and interact with a list of records, such as contacts, accounts, or custom objects." The condition logic is set to "All Conditions Are Met". A single condition is defined: "Event Source" equals "API". There is an "Add Condition" button at the bottom.

Track User's Session Level Security

Description of Example: Track when a user who doesn't have high assurance session-level security access (not logged in with two-factor authentication) queries any list view.

- **Event:** List View Event
- **Condition Logic:** Any Condition Is Met
- **Conditions:**
 - Session Level Equals LOW
 - Session Level Equals STANDARD
- **Notes:** Track when a user without high assurance executes a report (Report Event) or an API query (API Event) using the same condition in separate transaction security policies.

The screenshot shows the configuration for a List View Event. The event is set to "List View Event" with a description: "Track when users see and interact with a list of records, such as contacts, accounts, or custom objects." The condition logic is set to "Any Condition Is Met". Two conditions are defined, separated by an "OR" operator: "Session Level" equals "LOW" and "Session Level" equals "STANDARD". There is an "Add Condition" button at the bottom.

Block File Download

Description of Example: Detect and block a user from downloading a specific file.

- **Event:** File Event
- **Condition Logic:** Any Condition Is Met
- **Conditions:**
 - File Name Equals Asset.pdf

The screenshot shows the configuration for a File Event Store. The event is set to "File Event Store" with a description: "Track when a user downloads a file. Learn more...". The condition logic is set to "All Conditions Are Met (AND)". A single condition is defined: "File Name" equals "Assets.pdf". There is an "Add Condition" button at the bottom.

Use Custom Logic

Description of Example: Track when a user with a username in the @spy.mycompany.com domain queries all the records in a list view named SuperSecureListView.

- **Event:** List View Event
- **Condition Logic:** Custom Condition Logic is Met
- **Custom Condition Logic:** (1 OR 2) AND 3
- **Conditions:**
 - Scope Equals Everything
 - Name Equals SuperSecureListView
 - Username Ends With @spy.mycompany.com

• **Notes:**

* Event
List View Event Track when users see and interact with a list of records, such as contacts, accounts, or custom objects.

* Condition Logic
Custom Condition Logic Is Met

* Custom Condition Logic ⓘ
(1 OR 2) AND 3

	* Condition	* Operator	* Value	
1	Scope	Equals	Everything	🗑️
2	Name	Equals	SuperSecureListView	🗑️
3	Username	Ends With	@spy.mycompany.com	🗑️

+ Add Condition

Create an Enhanced Transaction Security Policy That Uses Apex

Use Setup to create an enhanced transaction security policy that uses Apex. You can specify an existing Apex class or create an empty class that you then code. The Apex class must implement the `TxnSecurity.EventCondition` interface.

You can create multiple policies for the same type of event, but we recommend that your policies and their actions don't overlap. If multiple policies with the same action for a given event execute when the event occurs, their order of execution is indeterminate.

1. From Setup, in the Quick Find box, enter *Transaction Security*, and then select **Transaction Security Policies**.
2. Click **New**, and then select **Apex**.
3. Click **Next**.
4. Select an event that your policy is built on.
For example, if you want to track API calls in your org, select **API Event**. If you want to monitor when users view or export reports, select **Report Event**. See [Enhanced Transaction Security](#) for the full list of available events.
5. Select the Apex class that implements your policy. If you haven't already created the class, select **New Empty Apex Class**.
6. Click **Next**.
7. Select the action that the policy performs when triggered.

The available actions vary depending on the event type. For more information, see [Enhanced Transaction Security Actions and Notifications](#).

 **Note:** The two-factor authentication action isn't available in the Salesforce mobile app, Lightning Experience, or via API for events. Instead, the block action is used. For example, if a two-factor authentication policy is triggered on a list view performed via the API, Salesforce blocks the API user.

8. If applicable, choose a block message or notification type and recipient.
9. Enter a name and description for your policy.
Your policy name must begin with a letter, not end with an underscore, and not contain two consecutive underscores.
10. Optionally, enable the policy.
If you chose to create an Apex class, don't enable the policy yet because you must first add code to the class.

11. Click **Finish**.

Your new policy appears in the Policies table. If you chose to create an Apex class, its name is the 25 characters of your policy name without spaces appended with the `EventCondition` string. If your policy is named "My Apex Class," your Apex class is auto-generated as `MyApexClassEventCondition`. The class is listed in the Apex Condition column.

12. Click the name of your Apex class if you want to edit it.

If you chose to create an Apex class, you must add the implementation code. Salesforce adds this basic code to get you started.

```
global class MyApexClassEventCondition implements TxnSecurity.EventCondition {

    public boolean evaluate(SObject event) {
        return false;
    }
}
```

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

USER PERMISSIONS

To view events:

- View Real-Time Event Monitoring Data

To view transaction security policies:

- View All Data

To create, edit, and manage transaction security policies:

- Customize Application

```
}

```

When you delete a transaction security policy that uses Apex, the implementation class isn't deleted. You can either delete this Apex class separately or reuse it in another policy.

Don't include DML statements in your Apex-based policies because they can cause errors. When you send a custom email via Apex during transaction policy evaluation, you get an error, even if the record isn't explicitly related to another record. For more information, see [Apex DML Operations](#) in the Apex Reference Guide.

[Enhanced Apex Transaction Security Implementation Examples](#)

Here are examples of implementing enhanced Apex transaction security.

[Asynchronous Apex Example](#)

When executing a transaction security policy, use an asynchronous Apex process to offload time-consuming operations, such as sending a notification email to an external recipient.

[Enhanced Transaction Security Apex Testing](#)

Writing robust tests is an engineering best practice to ensure that your code does what you expect and to find errors before your users and customers do. It's even more important to write tests for your transaction security policy's Apex code because it executes during critical user actions in your Salesforce org. For example, a bug in your LoginEvent policy that's not caught during testing can result in locking your users out of your org, a situation best avoided.

SEE ALSO:

[Apex Reference Guide: TxnSecurity.EventCondition Interface](#)

Enhanced Apex Transaction Security Implementation Examples

Here are examples of implementing enhanced Apex transaction security.

Login from Different IP Addresses

This example implements a policy that triggers when someone logs in from a different IP address in the past 24 hours.

EDITIONS

Available in: **Salesforce Classic** and **Lightning Experience**

Available in: **Enterprise**, **Unlimited**, and **Developer** Editions

Requires **Salesforce Shield** or **Salesforce Event Monitoring** add-on subscriptions.

```
global class MultipleLoginEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when LoginEvent loginEvent {
                return evaluate(loginEvent);
            }
            when null {
                return false;
            }
        }
    }
}
```

```

        }
        when else{
            return false;
        }
    }
}

private boolean evaluate(LoginEvent loginEvent) {
    AggregateResult[] results = [SELECT SourceIp
                                FROM LoginHistory
                                WHERE UserId = :loginEvent.UserId
                                AND LoginTime = LAST_N_DAYS:1
                                GROUP BY SourceIp];

    if(!results.isEmpty()) {
        return true;
    }
    return false;
}
}

```

Logins from a Specific IP Address

This example implements a policy that triggers when a session is created from a specific IP address.

```

global class SourceIpEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when LoginEvent loginEvent {
                return evaluate(loginEvent);
            }
            when null {
                return false;
            }
            when else{
                return false;
            }
        }
    }

    private boolean evaluate(LoginEvent loginEvent) {
        if (loginEvent.SourceIp.equals('1.1.1.1')) {
            return true;
        }
        return false;
    }
}

```

Data Export

This example implements a transaction security policy that triggers when more than 2,000 leads are either:

- Viewed in the UI
- Exported with a SOQL query
- Exported from a list view

- Exported from a report

```
global class LeadViewAndExportCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
            when ReportEvent reportEvent {
                return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
            }
            when ListViewEvent listViewEvent {
                return evaluate(listViewEvent.QueriedEntities, listViewEvent.RowsProcessed);
            }
            when null {
                return false;
            }
            when else{
                return false;
            }
        }
    }

    private boolean evaluate(String queriedEntities, Decimal rowsProcessed) {
        if(queriedEntities.contains('Lead') && rowsProcessed > 2000){
            return true;
        }
        return false;
    }
}
```

Confidential Data Access

This policy requires everyone to use two-factor authentication before accessing a specific report.

You can have sensitive, confidential data in your quarterly Salesforce reports. Make sure that teams that access the reports use two-factor authentication (2FA) for high assurance before they view this data. The policy makes 2FA a requirement, but you can't provide high-assurance sessions without a way for your teams to meet the 2FA requirements. As a prerequisite, first set up 2FA in your Salesforce environment.

This example highlights the capability of a policy to enforce 2FA for a specific report. The report defined here is any report with "Quarterly Report" in its name. Anyone accessing the report is required to have a high-assurance session using 2FA.

```
global class ConfidentialDataEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ReportEvent reportEvent {
                return evaluate(reportEvent);
            }
            when null {
                return false;
            }
            when else{
                return false;
            }
        }
    }
}
```

```

    }
  }
}

private boolean evaluate(ReportEvent reportEvent) {
  // Check if this is a quarterly report.
  if (reportEvent.Name.contains('Quarterly Report')) {
    return true;
  }
  return false;
}
}

```

Browser Check

This policy triggers when a user with a known operating system and browser combination tries to log in with another browser on a different operating system.

Many organizations have standard hardware and support specific versions of different browsers. You can use this standard to reduce the security risk for high-impact individuals by acting when logins take place from unusual devices. For example, your CEO typically logs in to Salesforce from San Francisco using a MacBook or Salesforce mobile application on an iPhone. When a login occurs from elsewhere using a Chromebook, it's highly suspicious. Because hackers do not necessarily know which platforms corporate executives use, this policy makes a security breach less likely.

In this example, the customer organization knows that its CEO uses a MacBook running OS X with the Safari browser. An attempt to log in using the CEO's credentials with anything else is automatically blocked.

```

global class AccessEventCondition implements TxnSecurity.EventCondition {
  public boolean evaluate(SObject event) {
    switch on event{
      when LoginEvent loginEvent {
        return evaluate(loginEvent);
      }
      when null {
        return false;
      }
      when else{
        return false;
      }
    }
  }
}

private boolean evaluate(LoginEvent loginEvent) {
  // If it's a Login attempt from our CEO's user account.
  if (loginEvent.UserId == '005x0000005VmCu'){
    // The policy is triggered when the CEO isn't using Safari on Mac OSX.
    if (!loginEvent.Platform.contains('Mac OSX') ||
        !loginEvent.Browser.contains('Safari')) {
      return true;
    }
  }
  return false;
}
}

```

Block Logins by Country

This policy blocks access by country.

Your organization has remote offices and a global presence but, due to international law, wants to restrict access to its Salesforce org.

This example builds a policy that blocks users logging in from North Korea. If users are in North Korea and use a corporate VPN, their VPN gateway would be in Singapore or the United States. They can log in successfully because Salesforce recognizes the VPN gateway and the internal U.S.-based company IP address.

```
global class CountryEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when LoginEvent loginEvent {
                return evaluate(loginEvent);
            }
            when null {
                return false;
            }
            when else{
                return false;
            }
        }
    }

    private boolean evaluate(LoginEvent loginEvent) {
        // Get the login's country.
        String country = String.valueOf(loginEvent.Country);

        // Trigger policy and block access for any user trying to log in from North Korea.

        if(country.equals('North Korea')) {
            return true;
        }
        return false;
    }
}
```

You can also restrict access to other values, like postal code or city.

Block an Operating System

This policy blocks access for anyone using an older version of the Android OS.

You're concerned about a specific mobile platform's vulnerabilities and its ability to capture screenshots and read data while accessing Salesforce. If the device is not running a security client, you could restrict access from device platforms that use operating systems with known vulnerabilities. This policy blocks devices using Android 5.0 and earlier.

```
global class AndroidEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when LoginEvent loginEvent {
                return evaluate(loginEvent);
            }
            when null {
                return false;
            }
        }
    }
}
```

```

        when else{
            return false;
        }
    }
}

private boolean evaluate(LoginEvent loginEvent) {
    String platform = loginEvent.Platform;
    // Block access from Android versions less than 5
    if (platform.contains('Android') && platform.compareTo('Android 5') < 0) {
        return true;
    }
    return false;
}
}

```

SEE ALSO:

[Apex Reference Guide: TxnSecurity.EventCondition Interface](#)

Asynchronous Apex Example

When executing a transaction security policy, use an asynchronous Apex process to offload time-consuming operations, such as sending a notification email to an external recipient.

This example has two parts. First, you create an asynchronous Apex class that uses an event within the execute method to invoke a callout or a DML operation. Second, you create a transaction security policy and modify the Apex class to implement TxnSecurity.EventCondition and TxnSecurity.AsyncCondition.

TxnSecurity.AsyncCondition enqueues the asynchronous Apex process when you trigger the transaction security policy.

 **Note:** Only DML operations and callouts are supported when you use asynchronous Apex with an enhanced transaction security policy.

Create Asynchronous Apex Class

In this section, you create an asynchronous Apex class that takes in an SObject. In this example, we use ApiEvent. Then you invoke a callout or a DML operation.

```

public class SimpleAsynchronousApex implements Queueable {
    private ApiEvent apiEvent;

    public SimpleAsynchronousApex(ApiEvent apiEvent) {
        this.apiEvent = apiEvent;
    }

    public void execute(QueueableContext context) {
        // Perform your callout to external validation service
        // or a DML operation
    }
}

```

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Create Policy

In this section, you create the transaction security policy, which modifies the Apex class associated with the policy. Then you create the `SimpleAsynchronousApex` object, pass in the `ApiEvent`, and enqueue the job.

```
global class SimpleApiEventCondition implements TxnSecurity.EventCondition,
TxnSecurity.AsyncCondition {
    public boolean evaluate(SObject event) {
        // Cast SObject to an ApiEvent object
        ApiEvent apiEvent = (ApiEvent) event;
        SimpleAsynchronousApex simpleAsynchronousApex = new SimpleAsynchronousApex(apiEvent);

        System.enqueueJob(simpleAsynchronousApex);
        return false;
        // In a typical implementation may return true if it triggers an action
    }
}
```

SEE ALSO:

[Apex Developer Guide: Queueable Apex](#)

[Apex Reference Guide: Apex Implementation Examples](#)

[Apex Developer Guide: Asynchronous Apex](#)

[Apex Developer Guide: Invoking Callouts Using Apex](#)

Enhanced Transaction Security Apex Testing

Writing robust tests is an engineering best practice to ensure that your code does what you expect and to find errors before your users and customers do. It's even more important to write tests for your transaction security policy's Apex code because it executes during critical user actions in your Salesforce org. For example, a bug in your `LoginEvent` policy that's not caught during testing can result in locking your users out of your org, a situation best avoided.

 **Warning:** Use API version 47.0 or later when writing Apex tests for enhanced transaction security policies.

When you test your Apex code by simulating a set of conditions, you are by definition writing unit tests. But writing unit tests isn't enough. Work with your business and security teams to understand all your use cases. Then create a comprehensive test plan that mimics your actual users' experience using test data in a sandbox environment. The test plan typically includes both manual testing and automated testing using external tools such as Selenium.

Let's look at some sample unit tests to get you started. Here's the Apex policy that we want to test.

```
global class LeadExportEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
            when ReportEvent reportEvent {
                return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
            }
            when ListViewEvent listViewEvent {
```

EDITIONS

Available in: **Salesforce Classic and Lightning Experience**

Available in: **Enterprise, Unlimited, and Developer Editions**

Requires **Salesforce Shield** or **Salesforce Event Monitoring add-on subscriptions**.

```

        return evaluate(listViewEvent.QueriedEntities, listViewEvent.RowsProcessed);
    }
    when null {
        return false;
    }
    when else {
        return false;
    }
}

private boolean evaluate(String queriedEntities, Decimal rowsProcessed){
    if (queriedEntities.contains('Lead') && rowsProcessed > 2000){
        return true;
    }
    return false;
}
}

```

Plan and Write Tests

Before we start writing tests, let's outline the positive and negative use cases that our test plan covers.

Table 11: Positive Test Cases

If the <code>evaluate</code> method receives...	And ...	Then the <code>evaluate</code> method returns...
An <code>ApiEvent</code> object	The <code>ApiEvent</code> has <code>Lead</code> in its <code>QueriedEntities</code> field and a number greater than 2000 in its <code>RowsProcessed</code> field	<code>true</code>
A <code>ReportEvent</code> object	The <code>ReportEvent</code> has <code>Lead</code> in its <code>QueriedEntities</code> field and a number greater than 2000 in its <code>RowsProcessed</code> field	<code>true</code>
A <code>ListViewEvent</code> object	The <code>ListViewEvent</code> has <code>Lead</code> in its <code>QueriedEntities</code> field and a number greater than 2000 in its <code>RowsProcessed</code> field	<code>true</code>
Any event object	The event doesn't have <code>Lead</code> in its <code>QueriedEntities</code> field and has a number greater than 2000 in its <code>RowsProcessed</code> field	<code>false</code>
Any event object	The event has <code>Lead</code> in its <code>QueriedEntities</code> field and has a number less than or equal to 2000 in its <code>RowsProcessed</code> field	<code>false</code>

If the evaluate method receives...	And ...	Then the evaluate method returns...
Any event object	The event doesn't have Lead in its QueriedEntities field and has a number less than or equal to 2000 in its RowsProcessed field	false

Table 12: Negative Test Cases

If the evaluate method receives...	And ...	Then the evaluate method returns...
A LoginEvent object	(no condition)	false
A null value	(no condition)	false
An ApiEvent object	The QueriedEntities field is null	false
A ReportEvent object	The RowsProcessed field is null	false

Here's the Apex testing code that implements all of these use cases.

```
/**
 * Tests for the LeadExportEventCondition class, to make sure that our Transaction Security
 * Apex
 * logic handles events and event field values as expected.
 */
@isTest
public class LeadExportEventConditionTest {

    /**
     * ----- POSITIVE TEST CASES -----
     */

    /**
     * Positive test case 1: If an ApiEvent has Lead as a queried entity and more than
     2000 rows
     * processed, then the evaluate method of our policy's Apex should return true.
     */
    static testMethod void testApiEventPositiveTestCase() {
        // set up our event and its field values
        ApiEvent testEvent = new ApiEvent();
        testEvent.QueriedEntities = 'Account, Lead';
        testEvent.RowsProcessed = 2001;

        // test that the Apex returns true for this event
        LeadExportEventCondition eventCondition = new LeadExportEventCondition();
        System.assert(eventCondition.evaluate(testEvent));
    }

    /**
     * Positive test case 2: If a ReportEvent has Lead as a queried entity and more than
```

```

2000 rows
  * processed, then the evaluate method of our policy's Apex should return true.
  **/
static testMethod void testReportEventPositiveTestCase() {
    // set up our event and its field values
    ReportEvent testEvent = new ReportEvent();
    testEvent.QueriedEntities = 'Account, Lead';
    testEvent.RowsProcessed = 2001;

    // test that the Apex returns true for this event
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assert(eventCondition.evaluate(testEvent));
}

/**
 * Positive test case 3: If a ListViewEvent has Lead as a queried entity and more
than 2000 rows
 * processed, then the evaluate method of our policy's Apex should return true.
 **/
static testMethod void testListViewEventPositiveTestCase() {
    // set up our event and its field values
    ListViewEvent testEvent = new ListViewEvent();
    testEvent.QueriedEntities = 'Account, Lead';
    testEvent.RowsProcessed = 2001;

    // test that the Apex returns true for this event
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assert(eventCondition.evaluate(testEvent));
}

/**
 * Positive test case 4: If an event does not have Lead as a queried entity and has
more
 * than 2000 rows processed, then the evaluate method of our policy's Apex
 * should return false.
 **/
static testMethod void testOtherQueriedEntityPositiveTestCase() {
    // set up our event and its field values
    ApiEvent testEvent = new ApiEvent();
    testEvent.QueriedEntities = 'Account';
    testEvent.RowsProcessed = 2001;

    // test that the Apex returns false for this event
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assertEquals(false, eventCondition.evaluate(testEvent));
}

/**
 * Positive test case 5: If an event has Lead as a queried entity and does not have
 * more than 2000 rows processed, then the evaluate method of our policy's Apex
 * should return false.
 **/
static testMethod void testFewerRowsProcessedPositiveTestCase() {

```

```

        // set up our event and its field values
        ReportEvent testEvent = new ReportEvent();
        testEvent.QueriedEntities = 'Account, Lead';
        testEvent.RowsProcessed = 2000;

        // test that the Apex returns false for this event
        LeadExportEventCondition eventCondition = new LeadExportEventCondition();
        System.assertEquals(false, eventCondition.evaluate(testEvent));
    }

/**
 * Positive test case 6: If an event does not have Lead as a queried entity and does
not have
 * more than 2000 rows processed, then the evaluate method of our policy's Apex
 * should return false.
**/
static testMethod void testNoConditionsMetPositiveTestCase() {
    // set up our event and its field values
    ListViewEvent testEvent = new ListViewEvent();
    testEvent.QueriedEntities = 'Account';
    testEvent.RowsProcessed = 2000;

    // test that the Apex returns false for this event
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assertEquals(false, eventCondition.evaluate(testEvent));
}

/**
 * ----- NEGATIVE TEST CASES -----
**/

/**
 * Negative test case 1: If an event is a type other than ApiEvent, ReportEvent, or
ListViewEvent,
 * then the evaluate method of our policy's Apex should return false.
**/
static testMethod void testOtherEventObject() {
    LoginEvent loginEvent = new LoginEvent();
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assertEquals(false, eventCondition.evaluate(loginEvent));
}

/**
 * Negative test case 2: If an event is null, then the evaluate method of our policy's
 * Apex should return false.
**/
static testMethod void testNullEventObject() {
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assertEquals(false, eventCondition.evaluate(null));
}

/**
 * Negative test case 3: If an event has a null QueriedEntities value, then the

```

```

evaluate method
    * of our policy's Apex should return false.
    **/
    static testMethod void testNullQueriedEntities() {
        ApiEvent testEvent = new ApiEvent();
        testEvent.QueriedEntities = null;
        testEvent.RowsProcessed = 2001;

        LeadExportEventCondition eventCondition = new LeadExportEventCondition();
        System.assertEquals(false, eventCondition.evaluate(testEvent));
    }

/**
 * Negative test case 4: If an event has a null RowsProcessed value, then the evaluate
method
 * of our policy's Apex should return false.
 **/
    static testMethod void testNullRowsProcessed() {
        ReportEvent testEvent = new ReportEvent();
        testEvent.QueriedEntities = 'Account, Lead';
        testEvent.RowsProcessed = null;

        LeadExportEventCondition eventCondition = new LeadExportEventCondition();
        System.assertEquals(false, eventCondition.evaluate(testEvent));
    }
}

```

Refine the Policy Code After Running the Tests

Let's say you run the tests and the `testNullQueriedEntities` test case fails with the error `System.NullPointerException: Attempt to de-reference a null object`. Great news, the tests identified an area of the transaction security policy that isn't checking for unexpected or null values. Because policies run during critical org operations, make sure that the policies fail gracefully if there's an error so that they don't block important functionality.

Here's how to update the `evaluate` method in the Apex class to handle those null values gracefully.

```

private boolean evaluate(String queriedEntities, Decimal rowsProcessed) {
    boolean containsLead = queriedEntities != null ? queriedEntities.contains('Lead')
    if (containsLead && rowsProcessed > 2000){
        return true;
    }
    return false;
}

```

We've changed the code so that before performing the `.contains` operation on the `queriedEntities` variable, we first check if the value is null. This change ensures that the code doesn't dereference a null object.

In general, when you encounter unexpected values or situations in your Apex code, you have two options. Determine what is best for your users when deciding which option to choose:

- Ignore the values or situation and return `false` so that the policy doesn't trigger.
- Fail-close the operation by returning `true`.

Advanced Example

Here's a more complex Apex policy that uses SOQL queries to get the profile of the user who is attempting to log in.

```
global class ProfileIdentityEventCondition implements TxnSecurity.EventCondition {

    // For these powerful profiles, let's prompt users to complete 2FA
    private Set<String> PROFILES_TO_MONITOR = new Set<String> {
        'System Administrator',
        'Custom Admin Profile'
    };

    public boolean evaluate(SObject event) {
        LoginEvent loginEvent = (LoginEvent) event;
        String userId = loginEvent.UserId;

        // get the Profile name from the current users profileId
        Profile profile = [SELECT Name FROM Profile WHERE Id IN
            (SELECT profileId FROM User WHERE Id = :userId)];

        // check if the name of the Profile is one of the ones we want to monitor
        if (PROFILES_TO_MONITOR.contains(profile.Name)) {
            return true;
        }

        return false;
    }
}
```

Here's our test plan for positive test cases:

- - If the user attempting to log in has the profile we're interested in monitoring, then the `evaluate` method returns `true`.
- If the user attempting to log in doesn't have the profile we're interested in monitoring, then the `evaluate` method returns `false`.

And here's our plan for negative test cases:

- - If querying for the Profile object throws an exception, then the `evaluate` method returns `false`.
- If querying for the Profile object returns null, then the `evaluate` method returns `false`.

Because every Salesforce user is always assigned a profile, there's no need to create a negative test for it. It's also not possible to create actual tests for the two negative test cases. We take care of them by updating the policy itself. But we explicitly list the use cases in our plan to make sure that we cover many different situations.

The positive test cases rely on the results of SOQL queries. To ensure that these queries execute correctly, we must also create some test data. Let's look at the test code.

```
/**
 * Tests for the ProfileIdentityEventCondition class, to make sure that our
 * Transaction Security Apex logic handles events and event field values as expected.
 */
@isTest
public class ProfileIdentityEventConditionTest {

    /**
     * ----- POSITIVE TEST CASES -----
     */
}
```

```

** /

/**
 * Positive test case 1: Evaluate will return true when user has the "System
 * Administrator" profile.
 **/
static testMethod void testUserWithSysAdminProfile() {
    // insert a User for our test which has the System Admin profile
    Profile profile = [SELECT Id FROM Profile WHERE Name='System Administrator'];
    assertOnProfile(profile.id, true);
}

/**
 * Positive test case 2: Evaluate will return true when the user has the "Custom
 * Admin Profile"
 **/
static testMethod void testUserWithCustomProfile() {
    // insert a User for our test which has the System Admin profile
    Profile profile = [SELECT Id FROM Profile WHERE Name='Custom Admin Profile'];
    assertOnProfile(profile.id, true);
}

/**
 * Positive test case 3: Evaluate will return false when user doesn't have
 * a profile we're interested in. In this case we'll be using a profile called
 * 'Standard User'.
 **/
static testMethod void testUserWithSomeProfile() {
    // insert a User for our test which has the System Admin profile
    Profile profile = [SELECT Id FROM Profile WHERE Name='Standard User'];
    assertOnProfile(profile.id, false);
}

/**
 * Helper to assert on different profiles.
 **/
static void assertOnProfile(String profileId, boolean expected){
    User user = createUserWithProfile(profileId);
    insert user;

    // set up our event and its field values
    LoginEvent testEvent = new LoginEvent();
    testEvent.UserId = user.Id;

    // test that the Apex returns true for this event
    ProfileIdentityEventCondition eventCondition = new
ProfileIdentityEventCondition();
    System.assertEquals(expected, eventCondition.evaluate(testEvent));
}

/**
 * Helper to create a user with the given profileId.
 **/
static User createUserWithProfile(String profileId){

```

```

// Usernames have to be unique.
String username = 'ProfileIdentityEventCondition@Test.com';

User user = new User(Alias = 'standt', Email='standarduser@testorg.com',
EmailEncodingKey='UTF-8', LastName='Testing', LanguageLocaleKey='en_US',
LocaleSidKey='en_US', ProfileId = profileId,
TimeZoneSidKey='America/Los_Angeles', UserName=username);
return user;
}
}

```

Let's handle the two negative test cases by updating the transaction security policy code to check for exceptions or null results when querying the Profile object.

```

global class ProfileIdentityEventCondition implements TxnSecurity.EventCondition {

// For these powerful profiles, let's prompt users to complete 2FA
private Set<String> PROFILES_TO_MONITOR = new Set<String> {
    'System Administrator',
    'Custom Admin Profile'
};

public boolean evaluate(SObject event) {
    try{
        LoginEvent loginEvent = (LoginEvent) event;
        String userId = loginEvent.UserId;

        // get the Profile name from the current users profileId
        Profile profile = [SELECT Name FROM Profile WHERE Id IN
            (SELECT profileId FROM User WHERE Id = :userId)];

        if (profile == null){
            return false;
        }

        // check if the name of the Profile is one of the ones we want to monitor
        if (PROFILES_TO_MONITOR.contains(profile.Name)) {
            return true;
        }
        return false;
    } catch(Exception ex){
        System.debug('Exception: ' + ex);
        return false;
    }
}
}

```

Best Practices for Writing and Maintaining Enhanced Transaction Security Policies

Transaction security policy management isn't always easy, especially when you have many policies. To make sure that your policies remain functional, write and maintain them using these best practices. Well-structured and tested policies keep your employees and customers connected, productive, and secure.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer Editions**

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Writing Policies

Use these general guidelines as you write your policies.

Know your users

Do your users use features that work best with certain browsers? Do they rely on mobile devices in the field? Have features that your users regularly access changed? Think about what your users experience during their day-to-day work, and write your policies with those behaviors in mind. Remember: Policies prevent activities that are genuinely out of bounds, and they must not prevent users from completing core job tasks.

Know what's coming

To check whether the features that your users rely on change, read the Salesforce release notes. Feature changes can sometimes cause your policies to behave unexpectedly.

Know your environments

Use sandbox environments to your advantage. Run your policies in a sandbox under conditions similar to your production org. Let policies run for 24 hours to see how they work. Use this feedback to evaluate how your policy functions in the conditions it has to work under.

Know your policies

To avoid confusion and lighten your maintenance load, create only one policy per event. Schedule regular policy maintenance and reviews to make sure that you don't have policies that counteract one another. Check the Salesforce release notes for feature updates that might change the way your policies behave.

Use these guidelines if you write an Apex-based policy rather than use Condition Builder.

Know your code

If you have an Apex developer in your organization, work with the developer as you write your policy. By consulting with someone who knows the ins and outs of Apex, you can team up to write robust and reliable policies and tests. If you don't have access to an Apex expert, learn about Apex by taking the Apex Basics Trailhead module or studying the Apex Developer Guide.

Know your limits

Because Apex runs in a multi-tenant environment, the Apex runtime engine strictly enforces limits. Enforcing limits ensures that runaway Apex code or processes don't monopolize shared resources. If some Apex code exceeds a limit, the associated governor issues a runtime exception that cannot be handled. Limits vary based on the event that the policy is based on. Construct your policies with these limits in mind. Read more about Apex Governors and Limits.

Testing Policies

Testing policies is the best way to make sure that you're crafting the right solution for your organization and your users.

- Try out your policies in a sandbox. Then deploy your security policy in a production org when you're certain your policy works.
- If you make far-reaching changes in your org, retest your policies to make sure that they are compatible with the changes you made. For example, if you create a workflow for field employees that generates a report, check all report event policies that could be affected.
- If your policy is Apex-based, follow Apex testing best practices.
- Run data silo tests. These tests run faster, produce easy-to-diagnose failures, and are more reliable.

Troubleshooting

Something is wrong with my policy. Where do I start?

Use the error message that your policy creates as a starting point. Check the Apex Developer Guide for advice on the error category.

My policy shuts down before it executes.

Policies don't execute if they take too long to perform all their actions. Streamline your policy, and make sure that it's within the metering limit.

I have multiple policies for the same event. What do I do?

In general, make only as many policies as you can manage and maintain. There's no limit on the number of policies you can create, but not all policies trigger. Policies are prioritized, and trigger in this order: block the operation, require multi-factor authentication, no action. If you have multiple policies for the same event, not all of those policies trigger. For example, let's say you have two policies for one event, but one policy blocks the operation and the second is set to require multi-factor authentication. The policy that blocks the user executes first and if it triggers, the other policy doesn't execute.

My policy isn't working. How do I debug it?

First, disable the policy and move it to a sandbox. You don't want a broken policy to cause problems for your colleagues or customers while you troubleshoot. Then evaluate whether the issue is with your policy settings or the Apex code if your policy is Apex-based.

- If you think your settings are the source of the problem, evaluate the policy's conditions and actions in your sandbox. Adjust the policy's settings, and test for the behaviors you want.
- If you suspect that the problem is with your Apex code, you can debug Apex using the Developer Console and debug logs.

I can't turn off my policy, and it's blocking my users in production. What do I do?

Check for known issues documented in Knowledge Articles or Known Issues. These resources explain issues that other customers experienced, along with functional workarounds. If that doesn't work, contact Salesforce.

Enhanced Transaction Security Metering

Transaction Security uses resource metering to help prevent malicious or unintentional monopolization of shared, multi-tenant platform resources. Metering prevents transaction security policy evaluations from using too many resources and adversely affecting your Salesforce org.

Salesforce meters transaction security policies for uniform resource use. If a policy request can't be handled within three seconds, a fail-close behavior occurs, and access is blocked. Transaction Security implements metering by limiting policy execution. If the elapsed execution time exceeds three seconds, the user's request is denied.

Here's an example of how metering works. Let's say your org has four LoginEvent policies set up with a notification action. A user triggers every policy. The first three execute within three seconds, but the final policy exceeds the three-second limit. Transaction Security stops processing the policies and fails closed, blocking the user's login request. Because the policy evaluations didn't finish, a notification isn't sent.

Bypass Metering-Related Blocking

Legitimate long-running processes, such as bulk API calls, can cause transaction security policy requests to take more than the allotted time. In these cases, metering initiates and blocks the user's action.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

If you encounter this situation regularly, you can prevent metering from blocking user actions with the `bypassMeteringBlock` field on the `EventSetting` metadata type. If all your transaction security policies specify no action, metering doesn't block user operations. If metering occurs, policy notifications aren't sent. Policies with block actions still block when triggered.

SEE ALSO:

[Metadata API Developer Guide: EventSettings](#)

Exempt Users from Transaction Security Policies

If you have transaction security policies that work well for most users, but not all, you can assign specific users the Exempt from Transaction Security user permission. Assign this permission only when transaction security policy metering regularly blocks business-critical actions. For example, assign it to users who make bulk or automated bulk API calls. You can assign this user permission to integration users or admins responsible for transaction security policies who you don't want to get blocked.

 **Note:** The Exempt from Transaction Security user permission doesn't apply to the `LoginEvent` type. Transaction Security policies can't check a user permission until after the user logs in.

1. Do one of the following:
 - a. From Setup, in the Quick Find box, enter *Permission Sets*, and then select **Permission Sets**.
 - b. From Setup, in the Quick Find box, enter *Profiles*, and then select **Profiles**.
2. Select a permission set or profile.
3. Depending on whether you're using permission sets or profiles, do one of the following:
 - a. In permission sets or the enhanced profile user interface, select a permission. In the Find Settings dialog box, enter *Exempt from Transaction Security*. Click **Edit**, select the option, and click **Save**.
 - b. In the original profile user interface, select a profile name, and then click **Edit**. Select **Exempt from Transaction Security**. Click **Save**.

Test and Troubleshoot Your New Enhanced Policy

If your enhanced transaction security policy isn't behaving as you expect, check out these testing and troubleshooting tips to diagnose the problem.

Test in a Sandbox

Always test a new policy in a sandbox before deploying it to production. While in your sandbox, create and enable the policy, and then try different actions to test whether it's executing as you expect.

For example, if you want your `ReportEvent` policy to block all report exports on leads, try different report operations to ensure that they're being blocked. For example:

- Run standard reports on leads.
- Create a custom report type on leads, and run reports that use that type.
- Execute report REST API queries on leads.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Check Your Policy Conditions

If your policy isn't working as you expect, it's possible that you added the wrong conditions. Event Manager is a great tool to troubleshoot policy conditions. When you enable storage or streaming for your event from the Event Manager UI, you can examine the field values for real events in your org. You can then compare these actual values with the values that you expect and see if they match.

For example, let's say you create a ReportEvent policy with the condition "QueriedEntities equals Lead." You then run a custom report type in your org that contains Lead objects. You expect the policy to trigger, but it doesn't. Try these steps to find the problem.

1. Enable storage for ReportEvent in Event Manager to view a history of the ReportEvents in your org.
2. Run your custom report type again so that a ReportEvent entry is stored.
3. From an API client such as Postman, query your ReportEvent event objects, and find the entry that corresponds to this recent run of the custom report type.
4. Check the value of the `QueriedEntities` field. Is it what you expected? If it isn't, change your condition. For example, if your custom report type is on more than just leads, the value of `QueriedEntities` is something like `Lead, Campaign, MyCustomObject__c`. In this case, change your policy condition to be "QueriedEntities *contains* Lead."

Add Automated Apex Tests

Automated Apex tests are a good way to find typos, logical flaws, and regressions in the Apex code for your new enhanced policy. In general, it's a best practice to write automated tests early in the development cycle. Testing ensures that you fix malfunctioning policies before they negatively affect your production users.

For example, the Lead Data Export Apex class contains a typo so that the condition tests for `Laed` instead of `Lead`. When you execute this Apex test, it fails, so you know that something is wrong.

```
/**
 * Tests for the LeadExportEventCondition class, to make sure that our Transaction Security
 * Apex
 * logic handles events and event field values as expected.
 */
@isTest
public class LeadExportEventConditionTest {

    /**
     * Test Case 1: If an ApiEvent has Lead as a queried entity and more than 2000 rows
     * processed, then the evaluate method of our policy's Apex should return true.
     */
    static testMethod void testApiEventPositiveTestCase() {
        // set up our event and its field values
        ApiEvent testEvent = new ApiEvent();
        testEvent.QueriedEntities = 'Account, Lead';
        testEvent.RowsProcessed = 2001;

        // test that the Apex returns true for this event
        LeadExportEventCondition eventCondition = new LeadExportEventCondition();
        System.assert(eventCondition.evaluate(testEvent));
    }
}
```

Add Apex Debug Logs

After creating and running Apex tests, you now know there's a problem in your Apex code, but you don't know what it is. Apex debug logs help you gain visibility into what your Apex class is doing so that you can fix the issue.

Let's update the Apex code for the enhanced Lead Data Export policy that currently has the unfortunate `Laed` typo with some `System.debug()` statements.

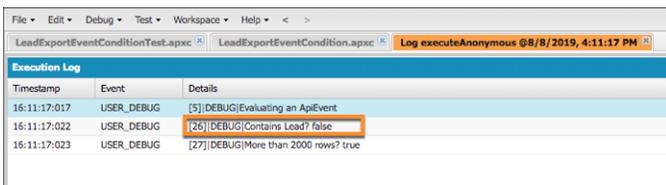
```
global class LeadExportEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                System.debug('Evaluating an ApiEvent');
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
            when ReportEvent reportEvent {
                System.debug('Evaluating a ReportEvent');
                return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
            }
            when null {
                System.debug('Evaluating null');
                return false;
            }
            when else {
                System.debug('Evaluating another event type: ' + event);
                return false;
            }
        }
    }

    private boolean evaluate(String queriedEntities, Decimal rowsProcessed){
        // pulling out our 2 conditions into variables
        // so that we can also use them for logging!
        boolean containsLead = queriedEntities.contains('Laed');
        boolean moreThan2000 = rowsProcessed > 2000;

        System.debug('Contains Lead? ' + containsLead);
        System.debug('More than 2000 rows? ' + moreThan2000);

        if (containsLead && moreThan2000){
            return true;
        }
        return false;
    }
}
```

Run the Apex test from the Developer Console, and view the debug logs that your Apex code generated. This example shows that the `QueriedEntities` field of the recent event doesn't contain a Lead. The highlighted debug log pinpoints the condition that didn't evaluate correctly. Now it's easy to examine your Apex code and find the typo.



Timestamp	Event	Details
16:11:17:017	USER_DEBUG	[5] DEBUG Evaluating an ApiEvent
16:11:17:022	USER_DEBUG	[26] DEBUG Contains Lead? false
16:11:17:023	USER_DEBUG	[27] DEBUG More than 2000 rows? true

If you want to see the debug output when a policy runs in a production environment, add a User Trace flag for the Automated User. The Automated User executes transaction security policies.



SETUP

Debug Logs

To specify the type of information that is included in debug logs, add trace flags and debug levels. Each trace flag includes a debug level, a start time, an end time, and a log type.

Trace flags set logging levels (such as for Database, Workflow, and Validation) for a user, Apex class, or Apex trigger for up to 24 hours.

- Select Automated Process from the drop-down list to set a trace flag on the automated process user. The automated process user runs background jobs, such as emailing Chatter invitations.
- Select Platform Integration from the drop-down list to set a trace flag on the platform integration user. The platform integration user runs processes in the background, and appears in audit fields of certain records, such as cases created by the Einstein Bot.
- Select User from the drop-down list to specify a user whose debug logs you'd like to monitor and retain.
- Select Apex Class or Apex Trigger from the drop-down list to specify the log levels that take precedence while executing a specific Apex class or trigger. Setting class and trigger trace flags doesn't cause logs to be generated or saved. Class and trigger trace flags override other logging levels, including logging levels set by user trace flags, but they don't cause logging to occur. If logging is enabled when classes or triggers execute, logs are generated at the time of execution.

[Configure your Debug Levels.](#)

Cancel Save

Traced Entity Type Automated Process ▾

Traced Entity Name Automated Process ⓘ 🔍

Start Date 8/11/2019 8:01 PM [8/11/2019 8:01 PM]

Expiration Date 8/11/2019 8:31 PM [8/11/2019 8:01 PM]

Debug Level ⓘ SFDC_DevConsole ⓘ 🔍 New Debug Level

Cancel Save

SEE ALSO:

[Manage Real-Time Event Monitoring Events](#)

[Execute Apex Tests](#)

[Apex Developer Guide: Debug Log](#)

[View Debug Logs](#)

[Set Up Debug Logging](#)

Threat Detection

Threat Detection uses statistical and machine learning methods to detect threats to your Salesforce org. While Salesforce identifies these threats for all Salesforce customers, you can view the information in the events with Threat Detection in Event Monitoring and investigate further if necessary.

Threat Detection identifies:

- If a user session is hijacked
 - When a user successfully logs in during an identified credential stuffing attack. Credential stuffing occurs when large-scale automated login requests use stolen user credentials to gain access to Salesforce.
 - Anomalies in a user's report views or exports
 - Anomalies in how users make API calls
-  **Note:** Not all third-party proxies pass network-related parameters, such as IP addresses, into Salesforce. Without network-related parameters, Salesforce doesn't detect all threats to these proxies.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Respond to Detected Threat Events

Use Threat Detection to plan and implement appropriate responses that keep your data safe. To help you respond in real time, Threat Detection events are compatible with transaction security policies and flows.

Use Transaction Security Policies to Monitor Threats

Create a transaction security policy on the Threat Detection events that generates email or in-app notifications when Salesforce detects a threat. After you investigate the detected threat, consider creating a policy to control users' behavior.

For example, you receive multiple ReportAnomalyEvents about a user who exported many more records of a report on Leads than usual. Because you created a transaction security policy on ReportAnomalyEventStore, you receive a notification each time this anomaly occurs. To further protect the Lead object, you can create a ReportEvent policy on the report to block users from exporting more than 10 rows.

Automate Responses with Platform Event-Triggered Flows

You can build flows to respond to anomalies detected on the ApiAnomalyEvent, CredentialStuffingEvent, ReportAnomalyEvent, and SessionHijackingEvent. For example, create flows that generate a case for a follow-up investigation, send an email to a security specialist, or deactivate an affected user pending further investigation.

Aggregate Detected Threats with Security Center

You can save time by aggregating information on detected threats across your entire Salesforce rollout in one place with the Threat Detection app in Security Center. For more information, see [Review Threat Detection Events](#)

Session Hijacking

Session Hijacking is a customer-focused attack where attackers try to steal information from using a client's access to a web application. In our case, this application is Salesforce. When a client successfully authenticates with Salesforce, they receive a session token. The attacker tries to hijack the client's session by obtaining their session token.

Credential Stuffing

Credential stuffing is a type of cyber attack that uses stolen account credentials. It's also known as "password spraying" or "credential spills". Attackers obtain large numbers of usernames and passwords through data breaches or other types of cyber attacks. They then use these credentials to gain unauthorized access to user accounts through large-scale automated login requests against a web application such as Salesforce.

Report Anomaly

An *anomaly* is any user activity that is sufficiently different from the historical activity of the same user. We use the metadata in Salesforce Core application logs about report generation and surrounding activities to build a baseline model of the historical activity. We then compare any new report generation activity against this baseline to determine if the new activity is sufficiently different to be called an anomaly. We don't look at the actual data that a user interacts with— we look at *how* the user interacts with the data.

API Anomaly

An *anomaly* is any user activity that is sufficiently different from the historical activity of the same user. We use the metadata in Salesforce Core application logs about API generation and surrounding activities to build a baseline model of the historical activity. We then compare any new API generation activity against this baseline to determine if the new activity is sufficiently different to be called an anomaly. We don't look at the actual data that a user interacts with— we look at *how* the user interacts with the data.

Guest User Anomaly

An *anomaly* is any user activity that is sufficiently different from the other users. We use the metadata in Salesforce Core application logs to build profiles representing guest users' data access activities. A guest user profile is identified as an anomaly when it exhibits data access behavior significantly different from the others.

View Threat Detection Events and Provide Feedback

Launch the Threat Detection app and view all the detected threats that occurred in your Salesforce org. Threats include anomalies in how users run reports, session hijacking attempts, and credential stuffing. Use the same app to easily provide feedback about the severity of a specific threat.

SEE ALSO:

[Platform Events Developer Guide: Real-Time Event Monitoring Objects](#)

[Platform Events Developer Guide: Subscribe to Platform Event Messages with Flows](#)

[Enhanced Transaction Security](#)

[How Salesforce Helps Protect You From Insider Threats](#)

[How Salesforce Helps Protect You From Credential Stuffers](#)

Session Hijacking

Session Hijacking is a customer-focused attack where attackers try to steal information from using a client's access to a web application. In our case, this application is Salesforce. When a client successfully authenticates with Salesforce, they receive a session token. The attacker tries to hijack the client's session by obtaining their session token.

The Real-Time Event Monitoring object SessionHijackingEvent addresses the "Man In The Browser" attack (MiTB), a type of session hijacking attack. In a MiTB attack, the attacker compromises the client's web application by first planting a virus like a Trojan proxy. The virus then embeds itself in the client's browser. And when the client accesses a web application such as Salesforce, the virus manipulates pages, collects sensitive information shared between the client and Salesforce, and steals information. These types of attacks are difficult for the client to detect.

Fortunately, Salesforce is ahead in this race with the bad guys and has mechanisms in place to detect MiTB attacks. When detected, Salesforce kills the session and any child sessions, logs out the user, and asks for multi-factor authentication. With this action, Salesforce helps prevent the attacker from performing any subsequent malicious activity with that user's session. This autonomous enforcement makes session hijacking costly for attackers and results in safer sessions for Salesforce customers.

All Salesforce customers get this threat mitigation. Event monitoring customers get granular visibility into these attacks. These customers can collect useful information about the attacks in real time and send notifications to other users in Salesforce.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

How Salesforce Detects Session Hijacking

To detect session hijacking attempts, Salesforce first uses browser fingerprinting to identify the device that a user has logged in from. If within a session, Salesforce sees a significant deviation in the browser fingerprint, there's probably unauthorized activity from a different device using the stolen legitimate session ID. Salesforce computes the session hijacking risk score for every pair of intra-session browser fingerprints. It then compares the score to an empirically determined threshold to detect anomalous user sessions in real time. If Salesforce detects an anomaly, it generates a `SessionHijackingEvent`.



Note: While Salesforce uses browser fingerprinting to identify a device, it doesn't use it to track a user. Salesforce uses the data only to detect suspicious behavior.

Features of the Browser Fingerprint

A browser fingerprint is a collection of features that together identify a device. Salesforce uses these features to build a model of the user's original browser fingerprint when they logged in. Salesforce uses this model to detect whether a user's session was hijacked.

Investigate Session Hijacking

Here are some tips for investigating a session hijacking attack.

SEE ALSO:

[Open Web Application Security Project: Session Hijacking Attack](#)

Features of the Browser Fingerprint

A browser fingerprint is a collection of features that together identify a device. Salesforce uses these features to build a model of the user's original browser fingerprint when they logged in. Salesforce uses this model to detect whether a user's session was hijacked.

Table 13: Features of Session Hijacking

Feature Name	Description	Example
window	The window size, in pixels, of the browser.	(750, 340)
userAgent	HTTP Header that contains information about the browser, operating system, version, and more.	Mozilla/5.0 (iPad; U; CPU iPhone OS 3_2 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Version/4.0.4 Mobile/7B314 Safari/531.21.10
timestamp	Timestamp of the captured event. Usually in Coordinated Universal Time (UTC) format.	2020-03-03T03:10:10Z
screen	The screen size, in pixels, of the browser.	(1050.0,1680.0)
plugins	JavaScript attribute that lists the activated browser plugins.	Chrome PDF Plugin:Portable

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Feature Name	Description	Example
		Document FormatChrome PDF Viewer
originApp	The origin app of the fingerprint.	Lightning
drm	Whether DRM (Digital Rights Management) is enabled.	0, 1
dnt	JavaScript attribute that indicates whether the user is requesting web sites and advertisers to not track them.	enabled
webSockets	Whether the browser used web sockets.	true
sessionStorage	Whether the browser used session storage.	true
platform	Browser-populated JavaScript attribute regarding the platform the browser is running on (window.navigator.platform).	iPad
localStorage	Whether local storage is used, extending beyond the duration of the session.	false
ipAddress	The IP address in the request.	96.43.144.26 or "Salesforce.com IP"
indexDb	Whether an indexed database is enabled for browser storage.	true
fonts	A hashed value of a list of browser fonts.	9wAt8lYAgO=
color	The color depth of the browser.	(24.0,24.0)

Investigate Session Hijacking

Here are some tips for investigating a session hijacking attack.

Start by querying these Real-Time Event Monitoring events that provide detailed information about the attack. In particular:

- SessionHijackingEvent and its storage equivalent SessionHijackingEventStore track when unauthorized users gain ownership of a Salesforce user's session with a stolen session identifier. To detect such an event, Salesforce evaluates how significantly a user's current browser fingerprint diverges from the previously known fingerprint. Salesforce uses a probabilistically inferred significance of change.

! **Important:** If the SessionHijackingEvent object contains a record, an attack occurred in the past and *Salesforce security has already taken care of the security issue*. You don't do anything other than investigate the attack for your own purposes.

- LoginEventStream (and its storage equivalent LoginEvent) tracks all login activity in your org.

For example, say that your org receives a SessionHijackingEvent. The first thing you do is look at relevant fields of the event to get basic information about the attack, such as:

- `Score`: A number from 0.0 to 1.0 that indicates how significantly the new browser fingerprint deviates from the previous one. The higher the number, the more likely a session hijacking attack occurred.
- `UserId`: The user's unique ID. Use this ID to query LoginEvent for more login information.
- `EventDate`: When this attack occurred.

EDITIONS

Available in: **Salesforce Classic** and **Lightning Experience**

Available in: **Enterprise**, **Unlimited**, and **Developer Editions**

Requires **Salesforce Shield** or **Salesforce Event Monitoring** add-on subscriptions.

- `SecurityEventData`: JSON field that contains the current and previous values of the browser fingerprint features that contributed the most to this anomaly detection. See [this table](#) for the full list of possible features.
- `Summary`: A text summary of the event.
- `Current-Previous` field pairs: These field pairs provide quick access to current and previous values for selected browser fingerprint features.
 - `CurrentIp` and `PreviousIp`: The current and previous IP address.
 - `CurrentPlatform` and `PreviousPlatform`: The current and previous operating system, such as Win32, MacIntel, or iPad.
 - `CurrentScreen` and `PreviousScreen`: The current and previous screen size in pixels, such as (900.0,1440.0).
 - `CurrentUserAgent` and `PreviousUserAgent`: The current and previous value of your browser's user agent that identifies the type of browser, version, operating system, and more. For example, Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
 - `CurrentWindow` and `PreviousWindow`: The current and previous window size in pixels, such as (1200.0,1920.0).

See the [API documentation](#) for the full list of fields.

This sample SOQL query returns these field values.

```
SELECT Score, UserId, EventDate, SecurityEventData, Summary
FROM SessionHijackingEventStore
```

Let's look at the `SecurityEventData` field a bit more closely because it contains the browser fingerprints that triggered this anomaly detection. Here's sample data:

```
[
  {
    "featureName": "userAgent",
    "featureContribution": "0.45 %",
    "previousValue": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
    like Gecko) Chrome/75.0.3770.142",
    "currentValue": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML,
    like Gecko) Chrome/76.0.3809.100 Safari/537.36."
  },
  {
    "featureName": "ipAddress",
    "featureContribution": "0.23 %",
    "previousValue": "201.17.237.77",
    "currentValue": "182.64.210.144"
  },
  {
    "featureName": "platform",
    "featureContribution": "0.23 %",
    "previousValue": "Win32",
    "currentValue": "MacIntel"
  },
  {
    "featureName": "screen",
    "featureContribution": "0.23 %",
    "previousValue": "(1050.0,1680.0)",
    "currentValue": "(864.0,1536.0)"
  },
  {
```

```
"featureName": "window",  
"featureContribution": "0.17 %",  
"previousValue": "1363x1717",  
"currentValue": "800x1200"  
}  
]
```

The sample JSON shows that many browser fingerprint features changed, including window, IP address, platform, and more. Salesforce concludes the user session was hijacked.

SEE ALSO:

[Platform Events Developer Guide: SessionHijackingEvent](#)

Credential Stuffing

Credential stuffing is a type of cyber attack that uses stolen account credentials. It's also known as "password spraying" or "credential spills". Attackers obtain large numbers of usernames and passwords through data breaches or other types of cyber attacks. They then use these credentials to gain unauthorized access to user accounts through large-scale automated login requests against a web application such as Salesforce.

Salesforce identifies a credential stuffing attack using a two-step process. First, it detects if a credential stuffing attack is taking place by analyzing the login traffic. In particular, we look for attackers who stuff multiple credentials in the same end-point or stuff the same user accounts by enumerating multiple passwords. Next we check the ratio of successful versus failed login traffic volume. If the volume exceeds a certain threshold, we use more fingerprint details to identify the affected user's profile.

When we detect a successful login from an endpoint that exhibits credential stuffing behavior, we pose an identity challenge to the affected user. If the user successfully completes that challenge, they are required to change their password before accessing Salesforce again.

All Salesforce customers get this threat mitigation. However, Event Monitoring customers can get granular visibility into these attacks using the CredentialStuffingEvent object. These customers can then collect useful information related to these events in real time and send notifications to other users in Salesforce.

[Investigate Credential Stuffing](#)

Here are some tips for investigating a credential stuffing attack.

EDITIONS

Available in: **Salesforce Classic and Lightning Experience**

Available in: **Enterprise, Unlimited, and Developer Editions**

Requires **Salesforce Shield** or **Salesforce Event Monitoring** add-on subscriptions.

Investigate Credential Stuffing

Here are some tips for investigating a credential stuffing attack.

Start by querying these Real-Time Event Monitoring events that provide detailed information about the attack. In particular:

- `CredentialStuffingEvent` and its storage equivalent `CredentialStuffingEventStore` track when a user successfully logs into Salesforce during an identified credential stuffing attack.
 - ❗ **Important:** If the `CredentialStuffingEvent` object contains a record, an attack occurred in the past and *Salesforce security has already taken care of the security issue*. You don't do anything other than investigate the attack for your own purposes.
- `LoginEventStream` and its storage equivalent `LoginEvent` track all login activity in your Salesforce org.

For example, say that your org receives a `CredentialStuffingEvent`. The first thing you do is look at relevant fields of the event to get basic information about the attack, such as:

- `UserId`: The user's unique ID. Use this ID to query `LoginEvent` for more login information.
- `EventDate`: When this attack occurred.
- `Summary`: A text summary of the event.

See the [API documentation](#) for the full list of fields.

This sample SOQL query returns these field values.

```
SELECT UserId, EventDate, Summary FROM CredentialStuffingEventStore
```

You can use this type of query to identify the users in your org that were affected by the credential stuffing attack. These users reused their org password in other websites or their password follows a common pattern and isn't strong enough. Educate your users on how they can create and manage strong passwords to protect your org.

Also consider improving your security with password protection. You can set password history, length, and complexity requirements. You can also specify what to do when a user forgets the password. Salesforce requires the use of multi-factor authentication (MFA) for all logins to the user interface — make sure MFA is enabled for all your users. Finally, investigate enabling Lightning Login for password-free logins.

SEE ALSO:

[Salesforce Help: Enable Lightning Login for Password-Free Logins](#)

[Trailhead: Educate Your Users to Help Protect Your Org](#)

[Salesforce Security Guide: Set Password Policies](#)

[Platform Events Developer Guide: CredentialStuffingEvent](#)

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Unlimited**, and **Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Report Anomaly

An *anomaly* is any user activity that is sufficiently different from the historical activity of the same user. We use the metadata in Salesforce Core application logs about report generation and surrounding activities to build a baseline model of the historical activity. We then compare any new report generation activity against this baseline to determine if the new activity is sufficiently different to be called an anomaly. We don't look at the actual data that a user interacts with— we look at *how* the user interacts with the data.

Training and Inference Steps

Similar to other machine learning or statistical models, our detection model has a familiar two-step process: a training step and an inference or detection step. As a customer, you don't perform either of these steps—Salesforce performs them for you. You only review the detection events generated by our detection mode and take further action if necessary.

Investigate Report Anomalies

It's often necessary to further investigate a report anomaly to either rule it out as benign or to determine if a data breach occurred.

Best Practices for Investigating Report Anomalies

Keep these tips and best practices in mind when you investigate unusual user behavior. They can help you find the information you require to make a well informed conclusion about your data's safety.

Report Anomaly Detection Examples

Here are several examples that illustrate how you can investigate anomalous report events thoroughly.

Training and Inference Steps

Similar to other machine learning or statistical models, our detection model has a familiar two-step process: a training step and an inference or detection step. As a customer, you don't perform either of these steps—Salesforce performs them for you. You only review the detection events generated by our detection mode and take further action if necessary.

Training Step

We extract various attributes—also known as *features*—using the metadata from the Salesforce application logs. We use metadata about report generation and surrounding activities over a period of 90 days. The actual list of features changes as the model improves.

Using these features, we build a model of the user's typical report generation activity. This step is called model training. We use the trained model to detect anomalies in the second step.

Inference (or Detection) Step

During the detection step, we look at every report generation activity for every user and extract the same set of features used to train the model. We then compare features against the model of the user's typical behavior and determine if the activity under consideration is sufficiently different.

Anomaly Score

We assign a numerical anomaly score to every report generation activity based on how different the activity is compared to the user's typical activity. The anomaly score is always a number from 0 through 100, and is often expressed as a percentage. A low anomaly score

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

indicates that the user's report generation activity is similar to the user's typical activity. A high anomaly score indicates that the user's report generation activity is different from the user's typical activity.

Critical Threshold

Every report generation event is assigned an anomaly score, but not all generation events are anomalies. We use a threshold to determine which report generation events are sufficiently different from a user's typical activity. Any event with an anomaly score above the critical threshold is considered an anomaly.

Investigate Report Anomalies

It's often necessary to further investigate a report anomaly to either rule it out as benign or to determine if a data breach occurred.

As a Shield customer, the Real-Time Event Monitoring events provide you with the required information to perform your investigation. In particular:

- `ReportAnomalyEvent` (and its storage equivalent `ReportAnomalyEventStore`) track when anomalies are detected about users running or exporting reports. These objects are the starting point of your investigation.
- `ReportEventStream` (and its storage equivalent `ReportEvent`) track in general when users run or export reports in your org. Use these objects to see real-time or historical report executions.
- `LoginEventStream` (and its storage equivalent `LoginEvent`) track all login activity in your org.

For example, say that your org receives a `ReportAnomalyEvent` that indicates a potential anomaly in a user's report execution. The first thing you do is look at relevant fields of the event to get basic information about the anomaly, such as:

- `Score`: A number that represents how much this user's report execution differed from their usual activity. The higher the number, the more it diverged.
- `UserId`: The user's unique ID.
- `EventDate`: When this anomaly occurred.
- `Report`: The report ID for which this anomaly was detected.
- `SecurityEventData`: JSON field that contains the features, such as row count or day of the week, that contributed the most to this anomaly detection. See [this table](#) on page 1134 for the full list of possible features.
- `Summary`: A text summary of the event.

See the [API documentation](#) for the full list of fields.

This sample SOQL query returns these field values.

```
SELECT Score, UserId, EventDate, Report, SecurityEventData, Summary
FROM ReportAnomalyEventStore
```

Let's look at the `SecurityEventData` field a bit more closely because it contains the contributing factors that triggered this anomaly detection. Here's sample data:

```
[
  {
    "featureName": "rowCount",
    "featureValue": "1937568",
    "featureContribution": "95.00 %"
  },
  {
```

EDITIONS

Available in: **Salesforce Classic and Lightning Experience**

Available in: **Enterprise, Unlimited, and Developer Editions**

Requires **Salesforce Shield** or **Salesforce Event Monitoring add-on subscriptions**.

```

"featureName": "autonomousSystem",
"featureValue": "Bigleaf Networks, Inc.",
"featureContribution": "1.62 %"
},
{
"featureName": "dayOfWeek",
"featureValue": "Sunday",
"featureContribution": "1.42 %"
},
{
"featureName": "userAgent",
"featureValue": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/76.0.3809.132 Safari/537.36}",
"featureContribution": "1.21 %"
},
{
"featureName": "periodOfDay",
"featureValue": "Evening",
"featureContribution": ".09 %"
},
{
"featureName": "averageRowSize",
"featureValue": "744",
"featureContribution": "0.08 %"
},
{
"featureName": "screenResolution",
"featureValue": "900x1440",
"featureContribution": "0.07 %"
}
]

```

The feature that contributed the most (95.00%) to this anomaly detection was `rowCount` with a value of 1937568. The feature indicates that the user viewed or exported a report that had 1,937,568 rows. But based on historical data, the user rarely views or exports so much data. The other features contributed much less to the score. For example, the user executed the report on Sunday, but this feature contributed only 1.42% to the overall score.

Now that you have the data, you can investigate further.

SEE ALSO:

[Training and Inference Steps](#)

[Platform Events Developer Guide: ReportAnomalyEvent](#)

[Platform Events Developer Guide: ReportEvent](#)

Best Practices for Investigating Report Anomalies

Keep these tips and best practices in mind when you investigate unusual user behavior. They can help you find the information you require to make a well informed conclusion about your data's safety.

Identify the involved user.

Keeping customer privacy in mind, we cannot access customer data or any data inside the reports. As a result, we can provide only the user ID of the user who generated the report that is marked as an anomaly. Use this user ID to locate the username and other details about the person associated with the detection event.

Field: `ReportAnomalyEvent.UserId`

Use the timestamp.

Our detection model already considers various features derived from the timestamp to determine report generation activity as anomalous or not. You can use this timestamp to narrow down the set of events you must review. You can also determine if the time of report generation was unusual for the user who generated the report.

Field: `ReportAnomalyEvent.EventDate`

Use contributing factors as a guide.

The contributing factors JSON output shows the [list of features](#) on page 1134 in descending order of contribution. As you start your investigation into the event logs, keep an eye out for the top contributing features. If these features look unusual, they can provide more evidence that confirms the anomaly or even indicate a possible data breach.

Field: `ReportAnomalyEvent.SecurityEventData`

Consider the anomaly in the context of the user's typical behavior.

Using the `ReportAnomalyEvent` field values, try to determine whether the user activity within the detection event is typical for the user. For example, consider if it's typical for a user to generate a report from the IP address provided.

Field: `ReportAnomalyEvent.SourceIp`

Consider the size of the report.

We consider the size of the report to determine if the report generation was anomalous. A user generating a larger report than usual can indicate an unauthorized data export attempt. For example, an attacker obtained unauthorized access to the user's account and exfiltrate as much data as possible before losing access. Alternatively, it could mean that a disgruntled employee is exfiltrating data for use beyond the needs of the employer.

Field: `ReportAnomalyEvent.SecurityEventData` (specifically the `rowCount` feature name)

Not all anomalies are malicious.

While some anomalies can indicate a malicious intent, other anomalies can be legitimate but unusual. Our detection model can produce detection events that are unusual but not malicious. For example, if an employee gets promoted to a new role and starts generating larger reports, our model can flag this behavior as anomalous.

SEE ALSO:

[Training and Inference Steps](#)

[Platform Events Developer Guide: ReportAnomalyEvent](#)

[Platform Events Developer Guide: ReportEvent](#)

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Unlimited**, and **Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Report Anomaly Detection Examples

Here are several examples that illustrate how you can investigate anomalous report events thoroughly.

Detection Event Isn't Anomalous

Jason is a sales data analyst who reports to the regional sales manager. It's Jason's job to generate reports for his manager's sales calls. On March 27, 2019, Jason's account was used to generate a report. Alia, the administrator for Jason's org, noticed a ReportAnomalyEvent about this report generation activity.

Detection Event Possibly Anomalous

Rob recently joined the company as a customer success representative. On Jan 15, 2019, Rob's account was used to generate a report. Tony, the org's Salesforce admin, noticed a ReportAnomalyEvent about this report generation activity.

Detection Event Is Definitely Anomalous but Maybe Not Malicious

Alice is a sales rep based in St. Louis. She's often on the road to meet with clients. When she travels, she generally, but not consistently, use her company's VPN to log into Salesforce.

Detection Event Is Confirmed Malicious

John, a sales rep based in San Francisco, often travels for work. He regularly downloads reports of his leads for his weekly sales presentations. John has access to 500-1,000 leads and his weekly report downloads typically contain 500–1,000 rows.

Detection Event Isn't Anomalous

Jason is a sales data analyst who reports to the regional sales manager. It's Jason's job to generate reports for his manager's sales calls. On March 27, 2019, Jason's account was used to generate a report. Alia, the administrator for Jason's org, noticed a ReportAnomalyEvent about this report generation activity.

The event contained this information.

ReportAnomalyEvent Field	Value
Score	97.9801
Sourcelp	96.43.144.30
EventDate	2019-03-27T07:45:07.192Z
UserId	00530000009M946
Report	00OD0000001IeVCMAy
SecurityEventData	(see next table)

The SecurityEventData field contained this information.

featureName	featureValue	featureContribution
rowCount	17234	60.2%
dayOfWeek	0	25.6%

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

featureName	featureValue	featureContribution
numberColumns	12	12.5%
numberFilters	11	1.04%
periodOfDay	Night	0.65%

Alia notices that this report had approximately 17k rows generated on a Sunday. She decides to investigate further. Using the `UserId` field value, Alia identifies Jason as the user. She then looks through Jason's past report generation activity using the `ReportEvent` event. She notices that Jason, a sales data analyst, generates reports of varying sizes, ranging from just a handful of rows to 20k rows. Alia also notices that Jason often accompanies his manager on road shows, which often involves working Sundays and nights.

Alia concludes that this detection event wasn't anomalous because the report generation activity is well within Jason's typical activity.

SEE ALSO:

[Platform Events Developer Guide: ReportAnomalyEvent](#)

[Platform Events Developer Guide: ReportEvent](#)

Detection Event Possibly Anomalous

Rob recently joined the company as a customer success representative. On Jan 15, 2019, Rob's account was used to generate a report. Tony, the org's Salesforce admin, noticed a `ReportAnomalyEvent` about this report generation activity.

The event contained this information.

ReportAnomalyEvent Field	Value
Score	96.4512
Sourcelp	96.43.144.28
EventDate	2019-01-15T07:45:07.192Z
UserId	00530000009M945
Report	00OD00000011eVCMAY
SecurityEventData	(see next table)

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

The `SecurityEventData` field contained this information.

featureName	featureValue	featureContribution
rowCount	46008	58.65%
userAgent	-	30.23%
averageRowSize	1534	6.58%
browserCodecs	-	2.33%

featureName	featureValue	featureContribution
acceptedLanguages	-	2.19%

Tony notices that the rowCount feature is a bit high for their org. The second-ranking feature is userAgent with a feature contribution of around 30%. This percentage indicates that this user agent is not common for their org. Tony investigates further and finds Rob with the UserId field. Tony notices that Rob is a relatively new employee. By looking at the ReportEvent events, Tony notices that Rob occasionally generates reports of 46k rows. Because Rob is a relatively new employee, Tony can't be certain whether this report matches Rob's typical activity pattern.

Tony concludes that this detection is possibly nomalous, although he doesn't take any threat mitigation actions now.

SEE ALSO:

[Platform Events Developer Guide: ReportAnomalyEvent](#)

[Platform Events Developer Guide: ReportEvent](#)

Detection Event Is Definitely Anomalous but Maybe Not Malicious

Alice is a sales rep based in St. Louis. She's often on the road to meet with clients. When she travels, she generally, but not consistently, use her company's VPN to log into Salesforce.

On July 27, 2015, Alice's account was used to generate a report from a relatively new IP address. Bob, the administrator for Alice's org, noticed a ReportAnomalyEvent about this report generation activity. The event contained this information.

ReportAnomalyEvent Field	Value
Score	95.0158
SourceIp	96.43.144.27
EventDate	2015-07-27T07:45:07.192Z
UserId	00530000009M944
Report	00OD0000001leVCMAY
SecurityEventData	(see next table)

EDITIONS

Available in: **Salesforce Classic and Lightning Experience**

Available in: **Enterprise, Unlimited, and Developer Editions**

Requires **Salesforce Shield** or **Salesforce Event Monitoring** add-on subscriptions.

The SecurityEventData field contained this information.

featureName	featureValue	featureContribution
autonomousSystem	Softbank Corp	73.4%
rowCount	50876	15.6%
userAgent	-	9.9%
numberFilters	11	0.81%
periodOfDay	Night	0.21%

Bob notices that the autonomous system—derived from the IP address—is the top-ranked feature with 73.4% feature contribution. This percentage indicates that Alice rarely uses this autonomous system. Bob also notices that the report has around 50k rows, which is not small for this org. Bob then uses the `UserId` to identify the user as Alice. By looking at the `ReportEvent` events, Bob notices that Alice typically generates reports containing 1,000–10,000 rows. But on rare occasions, Alice generated reports with more than 50k rows. The `userAgent` has a smaller feature contribution, which could be attributed to Alice using her mobile device less when she travels. The `numberFilters` and `periodOfDay` features have small feature contributions, and are therefore not important.

Because Alice rarely uses this autonomous system and the report is bigger than what Alice typically generates, Bob concludes that this report falls outside of typical activity. However, Bob is unable to verify whether Alice or an attacker committed this malicious act. He attempts to get more information on this incident before pursuing any threat mitigation actions.

SEE ALSO:

[Platform Events Developer Guide: ReportAnomalyEvent](#)

[Platform Events Developer Guide: ReportEvent](#)

Detection Event Is Confirmed Malicious

John, a sales rep based in San Francisco, often travels for work. He regularly downloads reports of his leads for his weekly sales presentations. John has access to 500-1,000 leads and his weekly report downloads typically contain 500–1,000 rows.

On May 12, 2019, however, a report of 996,262 rows was downloaded using John's account. Kate, the administrator for John's org, noticed a `ReportAnomalyEvent` about this report generation activity. The event contained this information.

ReportAnomalyEvent Field	Value
Score	95.48515
SourceIp	96.43.144.26
EventDate	2019-05-12T12:22:10.298+00:00
UserId	00530000009M943
Report	00OD0000001leVCMAY
SecurityEventData	(see next table)

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

The `SecurityEventData` field contained this information.

featureName	featureValue	featureContribution
rowCount	996262	99.37%
autonomousSystem	Starbucks Coffee Company	0.27%
dayOfWeek	Sunday	0.13%
averageRowSize	1507	0.06%
userAgent	-	0.02%

Kate starts an investigation to dig deeper. She uses the `UserId` to determine that the report was downloaded using John's account. She then searches the `ReportEvent` events for John and notices that he generates weekly reports, but they contain only 500–1,000 rows. The table shows that `rowCount` contributes nearly 100% to this anomaly. This feature contribution value is a numerical value that indicates the importance of `rowCount` in flagging this report generation activity as an anomaly. Because John has a consistent history of generating small reports (500–1,000 rows), a report with a million rows is a noticeable departure from that trend. This fact generates the high feature contribution value.

Upon further investigation, Kate discovers that John's account was hacked and the attacker escalated John's access privileges to access data for the entire sales team. As a result, the report contained sales leads for the entire sales team instead of only the sales leads assigned to John.

Kate concludes that this detection event is malicious and takes further threat mitigation actions.

SEE ALSO:

[Platform Events Developer Guide: ReportAnomalyEvent](#)

[Platform Events Developer Guide: ReportEvent](#)

API Anomaly

An *anomaly* is any user activity that is sufficiently different from the historical activity of the same user. We use the metadata in Salesforce Core application logs about API generation and surrounding activities to build a baseline model of the historical activity. We then compare any new API generation activity against this baseline to determine if the new activity is sufficiently different to be called an anomaly. We don't look at the actual data that a user interacts with— we look at *how* the user interacts with the data.

[Training and Inference Steps](#)

Similar to other machine learning or statistical models, our detection model has a familiar two-step process: a training step and an inference or detection step. As a customer, you don't perform either of these steps—Salesforce performs them for you. You only review the detection events generated by our detection mode and take further action if necessary.

[Investigate API Request Anomalies](#)

It's often necessary to further investigate an API request anomaly to either determine if a data breach occurred or to rule it out as benign.

[Best Practices for Investigating API Request Anomalies](#)

Keep these tips and best practices in mind when you investigate unusual user behavior. Find the information you require to make a well-informed evaluation of your data's safety.

[API Request Anomaly Detection Examples](#)

Here are several examples that illustrate how you can investigate anomalous API request events thoroughly.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Training and Inference Steps

Similar to other machine learning or statistical models, our detection model has a familiar two-step process: a training step and an inference or detection step. As a customer, you don't perform either of these steps—Salesforce performs them for you. You only review the detection events generated by our detection mode and take further action if necessary.

Training Step

We extract various attributes—also known as *features*—using the metadata from the Salesforce application logs. We use metadata about report generation and surrounding activities over a period of 90 days. The actual list of features changes as the model improves.

Using these features, we build a model of the user's typical report generation activity. This step is called model training. We use the trained model to detect anomalies in the second step.

Inference (or Detection) Step

During the detection step, we look at every report generation activity for every user and extract the same set of features used to train the model. We then compare features against the model of the user's typical behavior and determine if the activity under consideration is sufficiently different.

Anomaly Score

We assign a numerical anomaly score to every report generation activity based on how different the activity is compared to the user's typical activity. The anomaly score is always a number from 0 through 100, and is often expressed as a percentage. A low anomaly score indicates that the user's report generation activity is similar to the user's typical activity. A high anomaly score indicates that the user's report generation activity is different from the user's typical activity.

Critical Threshold

Every report generation event is assigned an anomaly score, but not all generation events are anomalies. We use a threshold to determine which report generation events are sufficiently different from a user's typical activity. Any event with an anomaly score above the critical threshold is considered an anomaly.

Investigate API Request Anomalies

It's often necessary to further investigate an API request anomaly to either determine if a data breach occurred or to rule it out as benign.

As a Shield customer, the Real-Time Event Monitoring events provide you with the required information to perform your investigation. In particular:

- `ApiAnomalyEvent` and its storage equivalent `ApiAnomalyEventStore` track anomalies in how users make API calls. These objects are the starting point of your investigation.
- `ApiEventStream` and its storage equivalent `ApiEvent` track user-initiated read-only API calls. Use these objects to see real-time or historical API executions.
- `LoginEventStream` (and its storage equivalent `LoginEvent`) track all login activity in your org.

For example, say that your org receives an `ApiAnomalyEvent` that indicates a potential anomaly in a user's API calls. The first thing you do is look at relevant fields of the event to get basic information about the anomaly, such as:

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

- **Score:** A number that represents how much this user's API activity differed from their usual activity. The higher the number, the more it diverged.
- **UserId:** The user's unique ID.
- **EventDate:** The time that the API request occurred.
- **SecurityEventData:** JSON field that contains the features, such as row count or day of the week, that contributed the most to this anomaly detection. See [this table](#) on page 1134 for the full list of possible features.
- **Summary:** A text summary of the event.

See the [API documentation](#) for the full list of fields.

This sample SOQL query returns these field values.

```
SELECT Score, UserId, EventDate, SecurityEventData, Summary
FROM ApiAnomalyEventStore
```

Let's look at the `SecurityEventData` field a bit more closely because it contains the contributing factors that triggered this anomaly detection. Here's sample data:

```
[
  {
    "featureName": "rowCount",
    "featureValue": "1937568",
    "featureContribution": "95.00 %"
  },
  {
    "featureName": "autonomousSystem",
    "featureValue": "Bigleaf Networks, Inc.",
    "featureContribution": "1.62 %"
  },
  {
    "featureName": "dayOfWeek",
    "featureValue": "Sunday",
    "featureContribution": "1.42 %"
  },
  {
    "featureName": "userAgent",
    "featureValue": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36",
    "featureContribution": "1.21 %"
  },
  {
    "featureName": "periodOfDay",
    "featureValue": "Evening",
    "featureContribution": ".09 %"
  },
  {
    "featureName": "averageRowSize",
    "featureValue": "744",
    "featureContribution": "0.08 %"
  },
  {
    "featureName": "screenResolution",
    "featureValue": "900x1440",
    "featureContribution": "0.07 %"
  }
]
```

```
}
]
```

The feature that contributed the most (95.00%) to this anomaly detection was `rowCount` with a value of 1937568. The feature indicates that the user viewed or exported a report that had 1,937,568 rows. But based on historical data, the user rarely views or exports so much data. The other features contributed much less to the score. For example, the user executed the report on Sunday, but this feature contributed only 1.42% to the overall score.

Now that you have the data, you can investigate further.

SEE ALSO:

[Platform Events Developer Guide: ApiAnomalyEvent](#)

[Platform Events Developer Guide: ApiEvent](#)

Best Practices for Investigating API Request Anomalies

Keep these tips and best practices in mind when you investigate unusual user behavior. Find the information you require to make a well-informed evaluation of your data's safety.

Identify the involved user.

Keeping customer privacy in mind, we can't access customer data or any data inside the reports. As a result, we can provide only the user ID of the user who generated the report that is marked as an anomaly. Use this user ID to locate the username and other details about the person associated with the detection event.

Field: `ApiAnomalyEvent.UserId`

Use the timestamp.

Our detection model already considers various features derived from the timestamp to determine report generation activity as anomalous or not. You can use this timestamp to narrow down the set of events you must review. You can also determine if the time of report generation was unusual for the user who generated the report.

Field: `ApiAnomalyEvent.EventDate`

Use contributing factors as a guide.

The contributing factors JSON output shows the [list of features](#) on page 1134 in descending order of contribution. As you start your investigation into the event logs, keep an eye out for the top contributing features. If these features look unusual, they can provide more evidence that confirms the anomaly or even indicate a possible data breach.

Field: `ApiAnomalyEvent.SecurityEventData`

Consider the anomaly in the context of the user's typical behavior.

Using the `ReportAnomalyEvent` field values, try to determine whether the user activity within the detection event is typical for the user. For example, consider if it's typical for a user to generate a report from the IP address provided.

Field: `ApiAnomalyEvent.SourceIp`

Consider the size of the report.

We consider the size of the report to determine if the report generation was anomalous. A user generating a larger report than usual can indicate an unauthorized data export attempt. For example, an attacker obtained unauthorized access to the user's account and exfiltrate as much data as possible before losing access. Or it could mean that a disgruntled employee is exfiltrating data for use beyond the needs of the employer.

Field: `ApiAnomalyEvent.SecurityEventData` (specifically the `rowCount` feature name)

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Not all anomalies are malicious.

While some anomalies can indicate a malicious intent, other anomalies can be legitimate but unusual. Our detection model can produce detection events that are unusual but not malicious. For example, if an employee gets promoted to a new role and starts generating larger reports, our model can flag this behavior as anomalous.

SEE ALSO:

[Platform Events Developer Guide: ApiAnomalyEvent](#)

[Platform Events Developer Guide: ApiEvent](#)

API Request Anomaly Detection Examples

Here are several examples that illustrate how you can investigate anomalous API request events thoroughly.

[API Detection Event Isn't Anomalous](#)

Jason, a developer, uses APIs to query an Account object on a Sunday. He retrieves 10,000 records.

[API Detection Event Possibly Anomalous](#)

Rob, a relatively new Sales Operation Lead, uses an API to query the Opportunity object and extracts 10 million records. He previously queried the same object using a different browser and from a different IP address.

[API Detection Event Is an Anomaly but Isn't Clearly Malicious](#)

Alice is a sales rep based in St. Louis. She's often on the road to meet with clients. When she travels, she generally, but not consistently, uses her company's VPN to log into Salesforce.

[API Detection Event Is Confirmed Malicious](#)

Alan, a Salesforce user, employs an API to query the Opportunity object and extracts 10 million records. It's the first time that Alan queries the Opportunity object and uses this IP address to log in.

API Detection Event Isn't Anomalous

Jason, a developer, uses APIs to query an Account object on a Sunday. He retrieves 10,000 records.

The event contains this information.

APIAnomalyEvent Field	Value
Score	.5801
Sourcelp	96.43.144.30
EventDate	2020-03-27T07:45:07.192Z
UserId	00530000009M946
SecurityEventData	(see next table)

The `SecurityEventData` field contains this information.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

featureName	featureValue	featureContribution
rowCount	1937568	95.00%
autonomousSystem	Bigleaf Networks, Inc.	1.62%
dayOfWeek	Sunday	1.42%
userAgent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36}	1.21%
periodOfDay	Evening	0.09%
averageRowSize	744	0.08%
screenResolution	900x1440	0.07%

Alia, the Salesforce admin, notices that 10,000 records were retrieved from an Account object on a Sunday. She investigates further. Using the `userId` field value, Alia identifies Jason as the user. She then looks through Jason's past activity. She notices that Jason, a developer, retrieves records of varying amounts, ranging from just a handful to 20,000 records. Alia also notices in the `dayOfWeek` and `periodOfDay` features that Jason often works Sundays and nights.

Alia concludes that this detection event wasn't anomalous because the activity is well within Jason's typical activity.

SEE ALSO:

[Platform Events Developer Guide: ApiAnomalyEvent](#)

[Platform Events Developer Guide: ApiEvent](#)

API Detection Event Possibly Anomalous

Rob, a relatively new Sales Operation Lead, uses an API to query the Opportunity object and extracts 10 million records. He previously queried the same object using a different browser and from a different IP address.

The event contains this information.

APIAnomalyEvent Field	Value
Score	.7212
Sourcelp	96.43.144.28
EventDate	2019-01-15T07:45:07.192Z
UserId	00530000009M945
SecurityEventData	(see next table)

The `SecurityEventData` field contains this information.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

featureName	featureValue	featureContribution
rowCount	1937568	95.00%
autonomousSystem	Bigleaf Networks, Inc.	1.62%
dayOfWeek	Sunday	1.42%
userAgent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36}	29.21%
periodOfDay	Evening	0.09%
averageRowSize	744	0.08%
screenResolution	900x1440	0.07%

Tony, the security auditor, notices that the `rowCount` feature is a bit high for their Salesforce org. The second-ranking feature is `userAgent` with a feature contribution of close to 30%. This percentage indicates that this user agent, or browser, isn't common for their org. Tony finds Rob with the `userId` field. Tony notices that Rob is a relatively new employee. By looking at the `<need field or feature name>` events, Tony notices that Rob used a different browser and IP address in the past. Because Rob is a relatively new employee, Tony can't be certain whether this report matches Rob's typical activity pattern.

Tony concludes that this detection is possibly anomalous.

SEE ALSO:

[Platform Events Developer Guide: ApiAnomalyEvent](#)

[Platform Events Developer Guide: ApiEvent](#)

API Detection Event Is an Anomaly but Isn't Clearly Malicious

Alice is a sales rep based in St. Louis. She's often on the road to meet with clients. When she travels, she generally, but not consistently, uses her company's VPN to log into Salesforce.

On July 27, 2020, Alice's account was used to query an object from a relatively new IP address. Bob, the administrator for Alice's Salesforce org, noticed a `APIAnomalyEvent` about this report generation activity. The event contained this information.

APIAnomalyEvent Field	Value
Score	.8671
SourceIp	96.43.144.27
EventDate	2015-07-27T07:45:07.192Z
UserId	00530000009M944
SecurityEventData	(see next table)

The `SecurityEventData` field contains this information.

EDITIONS

Available in: **Salesforce Classic and Lightning Experience**

Available in: **Enterprise, Unlimited, and Developer Editions**

Requires **Salesforce Shield** or **Salesforce Event Monitoring add-on subscriptions**.

featureName	featureValue	featureContribution
rowCount	50568	95.00%
autonomousSystem	Bigleaf Networks, Inc.	73.4%
dayOfWeek	Sunday	1.42%
userAgent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36}	29.21%
periodOfDay	Evening	0.09%
averageRowSize	744	0.08%
screenResolution	900x1440	0.07%

Bob, the Salesforce admin, notices that the autonomous system—derived from the IP address—is the top-ranked feature with 73.4% feature contribution. This percentage indicates that Alice rarely uses this autonomous system. Bob also notices that the `rowCount` has around 50,000 rows, which isn't small for this org. Bob then uses the `userId` to identify the user as Alice. By looking at the `<need event name here>` events, Bob notices that Alice typically generates reports containing 1,000–10,000 rows. But on rare occasions, Alice generated reports with more than 50,000 rows. The `userAgent` has a smaller feature contribution, which could be attributed to Alice using her mobile device less when she travels. The `numberFilters` and `periodOfDay` features have small feature contributions, and are therefore not important.

Because Alice rarely uses this autonomous system and the report is larger than reports Alice typically generates, Bob concludes that this report falls outside of typical activity. But Bob is unable to verify whether Alice or an attacker committed this malicious act. He attempts to get more information on this incident.

SEE ALSO:

[Platform Events Developer Guide: ApiAnomalyEvent](#)

[Platform Events Developer Guide: ApiEvent](#)

API Detection Event Is Confirmed Malicious

Alan, a Salesforce user, employs an API to query the Opportunity object and extracts 10 million records. It's the first time that Alan queries the Opportunity object and uses this IP address to log in.

The event contains this information.

APIAnomalyEvent Field	Value
Score	.95851
Sourcelp	96.43.144.26
EventDate	2019-05-12T12:22:10.298+00:00
UserId	00530000009M943
SecurityEventData	(see next table)

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

The `SecurityEventData` field contains this information.

featureName	featureValue	featureContribution
rowCount	1937568	95.00%
autonomousSystem	Bigleaf Networks, Inc.	1.62%
dayOfWeek	Sunday	1.42%
userAgent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36}	29.21%
periodOfDay	Evening	0.09%
averageRowSize	744	0.08%
screenResolution	900x1440	0.07%

Kate, the security auditor, starts an investigation. She uses the `USERID` to determine that Alan's account was used to query the Opportunity object. She then searches the events for Alan and notices that he's never queried the Opportunity object. The table shows that `rowCount` contributes nearly 100% to this anomaly. This feature contribution value is a numerical value that indicates the importance of `rowCount` in flagging this report generation activity as an anomaly. Because Alan has no history of generating small reports (500–1,000 rows), a report with a million rows is a noticeable departure from that trend. This fact generates the high feature contribution value.

Kate next discovers that Alan's account was hacked and the attacker escalated Alan's access privileges to access data for the entire sales team. As a result, the records contain sales leads for the entire sales team instead of only the sales leads assigned to Alan.

Kate concludes that this detection event is malicious.

SEE ALSO:

[Platform Events Developer Guide: ApiAnomalyEvent](#)

[Platform Events Developer Guide: ApiEvent](#)

Guest User Anomaly

An *anomaly* is any user activity that is sufficiently different from the other users. We use the metadata in Salesforce Core application logs to build profiles representing guest users' data access activities. A guest user profile is identified as an anomaly when it exhibits data access behavior significantly different from the others.

[Investigate Guest User Anomalies](#)

It's often necessary to further investigate a guest user anomaly to determine if a data breach occurred or to rule it out as benign.

[Best Practices for Investigating Guest User Anomalies](#)

Keep these tips in mind when you investigate unusual user behavior. Find the information that you require to make a well-informed evaluation of your data's safety.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Unlimited**, and **Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Investigate Guest User Anomalies

It's often necessary to further investigate a guest user anomaly to determine if a data breach occurred or to rule it out as benign.

As a Shield customer, the Real-Time Event Monitoring events provide you with the required information to perform your investigation. In particular:

- GuestUserAnomalyEvent and its storage equivalent GuestUserAnomalyEventStore. This entity helps detect data access anomalies caused by guest user misconfiguration. These objects are the starting point of your investigation.

For example, say that your org receives a GuestUserAnomalyEvent that indicates a potential anomaly in a guest user's data access attempt. The first thing you do is look at relevant fields of the event to get basic information about the anomaly, such as:

Field	Description
RequestedEntities	Objects that are queried by the guest user. For example: <pre>[" Topic \"]</pre>
Score	Specifies how significantly the guest user behavior deviates from the other guest users. It's formatted as a number between 0 and 1.
SoqlCommands	SOQL commands run by the guest user. For example: <pre>["SELECT Name, Description, CreatedDate, Id, SystemModstamp FROM Topic ORDER BY Name ASC, Id ASC LIMIT 1000\", \"SELECT COUNT() FROM Topic LIMIT 2000\"]</pre>
Summary	A text summary of the threat that caused this event to be created. The summary lists the browser fingerprint features that most contributed to the threat detection along with their contribution to the total score. For example: <pre>Anomaly in SelectData Controller behavior</pre>
TotalControllerEvents	The number of times controllers were triggered.
UserAgent	User Agent for this event. For example: <pre>Mozilla/5.0 (Macintosh; Intel Mac OS X 11_2_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36</pre>

See the [API Documentation](#) for a full list of fields.

Now that you have the data, you can investigate further.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Unlimited**, and **Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Best Practices for Investigating Guest User Anomalies

Keep these tips in mind when you investigate unusual user behavior. Find the information that you require to make a well-informed evaluation of your data's safety.

We recommend that you review these following settings.

- **Organization Wide Default (OWD) Sharing Settings:**
 - All Standard & Custom Objects having Default External access as Public Read or Public Read/Write (for example, Accounts)
 - All Standard & Custom Objects having Default External access as Controlled by Parent, as the permission follows the parent objects (for example, Contacts).
- **Guest User Profiles:**
 - Any Create, Read, Update, Delete (CRUD) access owned by each standard or custom object within guest user profiles
 - Ensure the API Enabled and Access Activities checkboxes are unchecked.

To generate a report showing your current Guest User access and permissions, please use the Authenticated and Guest User Access Report and Monitoring app, which can be found in the AppExchange marketplace. To ensure that you aren't inadvertently permitting guest users access to your data in this manner, we suggest reviewing these best practices:

Org Settings

1. Ensure that List Views are shared only with certain groups or set to private.
2. Set internal and external organization-wide sharing defaults (OWD) to 'private' on all objects with non-public data.
3. Alternate sharing models can be permitted with proper justification. For example, adequate restrictions at the create, read, update, and delete [CRUD] level.
4. Set all sharing rules to not share any data with the Site Guest User.
5. Restrict access to @AuraEnabled Apex Methods for Guest and Portal Users Based on User Profile.

Site Guest User Profiles

1. Review field-level security for each object.
2. Configure Sharing Rules and Permission sets to not open access for custom or standard objects.
3. Ensure that all active profiles have no access to standard or custom objects that could contain personal information, per the [Best Practices and Considerations When Configuring the Guest User Profile](#).
4. Confirm that Object access, and the API Enabled and Access Activities checkboxes are unchecked.
5. Transfer ownership of sensitive records created by the Site Guest User profile to an internal user by following the steps outlined in [Assign Records Created by Guest Users to a Default User in the Org documentation](#).
6. Ensure that ownership of all existing records is transferred to an internal user.

Additional Steps

1. Remove guest user visibility in Communities/Experience Cloud by disabling the Let guest users see other members of this site checkbox under Setup. From Setup, go to Digital Experiences > All Sites > Workspaces > Administration > Preferences.
2. Review any custom Apex code:
 - Check for public API methods returning data, and confirm methods can't be used to exfiltrate object records.
 - Enforce field-level security for all Apex classes.
 - Ensure that all controllers are respecting the permissions of the current user.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

3. Keep JavaScript libraries in static resources continually updated to the latest security patch
4. By default, unassigned files are public. As a best practice, set up a trigger to assign an owner to files uploaded by guest users. You can restrict file upload size or type using community file moderation.

View Threat Detection Events and Provide Feedback

Launch the Threat Detection app and view all the detected threats that occurred in your Salesforce org. Threats include anomalies in how users run reports, session hijacking attempts, and credential stuffing. Use the same app to easily provide feedback about the severity of a specific threat.

[Make the Threat Detection App Visible to Users](#)

Before you can view the Threat Detection events in Salesforce and provide feedback, you must make the app visible to users. You also specify which of the four tabs are visible to different user profiles.

[View Events and Provide Feedback](#)

View recent or all Threat Detection events using the Threat Detection app in the Salesforce UI. The displayed events are stored in their corresponding storage objects: ReportAnomalyEventStore, SessionHijackingEventStore, and CredentialStuffingEventStore. Associate a feedback object with a particular event to record the severity of the threat, such as Malicious or Not a Threat.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

USER PERMISSIONS

User Permissions Needed

To view the Threat Detection events:

- View Threat Detection Events

Make the Threat Detection App Visible to Users

Before you can view the Threat Detection events in Salesforce and provide feedback, you must make the app visible to users. You also specify which of the four tabs are visible to different user profiles.

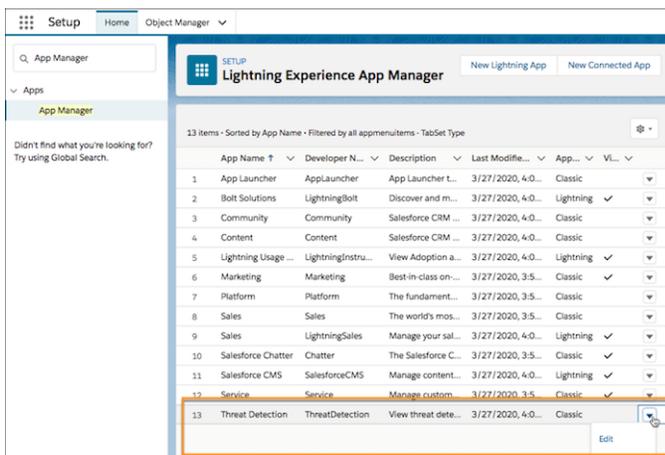
1. Use Event Manager to enable streaming and storage for the three Threat Detection events: ReportAnomalyEvent, SessionHijackingEvent, and CredentialStuffingEvent.
2. Create a permission set that's associated with the Salesforce license.
3. Edit the System Permissions page of your permission set and enable the **View Threat Detection Events** permission.
4. Assign the permission set to the user who administers the Threat Detection app.

Salesforce recommends that you create a profile specifically for security administrators who are responsible for managing threat detections. For example, create a profile called Threat Detection Administrator. Then assign the permission set to a user with the Threat Detection Administrator profile.

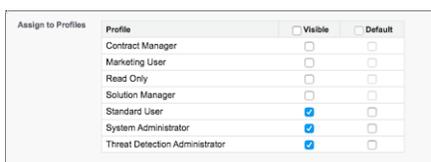
5. Edit the Tab Settings of each user profile that uses the Threat Detection app and specify the visibility of the four tabs. The four tabs are named Report Anomaly Event Store, Session Hijacking Event Store, Credential Stuffing Event Store, and Threat Detection Feedback.

For example, system administrators usually access everything in the UI, so set the visibility of all four tabs to Default On for the System Administrator profile. If you created a Threat Detection Administrator profile, set the same visibility. If you don't want standard users to view feedback, set the visibility of Threat Detection Feedback for the Standard User profile to Tab Hidden.

6. In Setup, navigate to the Lightning Experience App Manager by entering *App Manager* in the quick search box.
7. Edit the Threat Detection app by selecting **Edit** in the dropdown box to the right of the app.



8. In the Assign to Profiles section, select the profiles for which the Threat Detection app is visible.



9. Save your changes.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

USER PERMISSIONS

User Permissions Needed

To view the Threat Detection events:

- View Threat Detection Events

The Threat Detection app is now visible to selected users.

SEE ALSO:

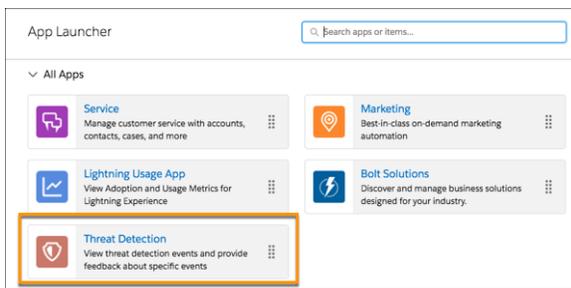
- [Salesforce Help: Monitor Streaming Events with Event Manager](#)
- [Salesforce Help: Permission Sets](#)
- [Salesforce Help: App and System Settings in Permission Sets](#)
- [Salesforce Help: View and Edit Tab Settings in Permission Sets and Profiles](#)

View Events and Provide Feedback

View recent or all Threat Detection events using the Threat Detection app in the Salesforce UI. The displayed events are stored in their corresponding storage objects: ReportAnomalyEventStore, SessionHijackingEventStore, and CredentialStuffingEventStore. Associate a feedback object with a particular event to record the severity of the threat, such as Malicious or Not a Threat.

By default, the Threat Detection app isn't visible in Salesforce. If necessary, make it visible as described in [Make the Threat Detection App Visible to Users](#).

1. From App Launcher, click **Threat Detection**.



2. Click the tabs for list views of recent or all events stored in the GuestUserAnomalyEventStore, ReportAnomalyEventStore, SessionHijackingEventStore, ApiAnomalyEventStore, or CredentialStuffingEventStore objects.
3. To view an event's details, click its link. Information such as the date the event occurred, its score, and a summary of the event is displayed.

Each type of event displays other details appropriate to the type of detected threat. For example, the Session Hijacking Event Store tab displays previous and current browser fingerprint information. The Report Anomaly Event Store tab displays the report ID associated with the detected threat.

Click Related to view the associated feedback, if any.

4. Click Provide Feedback to specify whether a specific detected threat is Malicious, Suspicious, Not a Threat, or Unknown. You can associate only one feedback object with each event. If you try to provide more than one feedback object, you get an error. If the severity of a threat changes after you provided feedback, edit the response.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Unlimited**, and **Developer** Editions

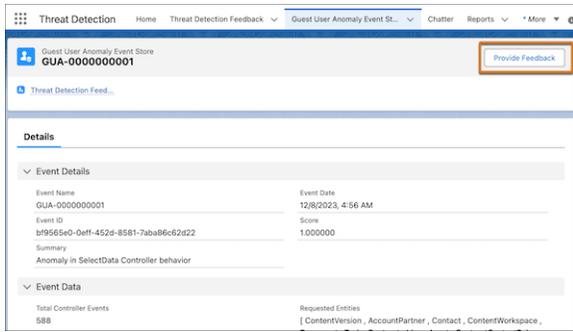
Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

USER PERMISSIONS

User Permissions Needed

To view the Threat Detection events:

- View Threat Detection Events



SEE ALSO:

[Platform Events Developer Guide: Real-Time Event Monitoring Objects](#)

Explore Event Log File Data using the Event Log File Browser (Beta)

The Event Log File Browser (beta) in Setup gives you quick access to event log files so you can explore and download all of your Event Log File data.

Note: This feature is a Beta Service. Customer may opt to try such Beta Service in its sole discretion. Any use of the Beta Service is subject to the applicable Beta Services Terms provided at [Agreements and Terms](#).

Discover Event Log Files

Use ELF browser (beta) to sort and explore Event Log Files by type, log date, log file length, and more. Easily filter by date and event type to find the data you need. You can access ELF Browser (beta) directly from Setup.

Download Event Log Files directly from ELF Browser

Download Event Log File data by selecting a date range, clicking the dropdown button to the right of the event log file, and selecting **Download as CSV File**.

Alternatively, use the File Download servlet by adding `/servlet/servlet.FileDownload?file=<ELF_ID_NUMBER>` after your org URL. For example, `https://mycompany.my.salesforce.com/servlet/servlet.FileDownload?file=0ATRM000000dcbH0A0`. The file download begins automatically.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Unlimited**, and **Developer Editions**

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Event Log Files
Explore and download event log file data.

Start Date: [Calendar Icon] End Date: [Calendar Icon] Event Type: All Interval: All **Apply**

8 events - Sorted by Log Date

Event Lo...	Event Type	Log Da...	Log File L...	Sequence	Interval	
0ATRM00000...	Aura Request	December 01,...	45	0	Daily	Download as CSV File
0ATRM00000...	Flow Execution	December 01,...	0	0	Daily	
0ATRM00000...	Lightning Inte...	December 01,...	20	0	Daily	
0ATRM00000...	Lightning Log...	December 01,...	1	0	Daily	
0ATRM00000...	Lightning Pag...	December 01,...	3	0	Daily	
0ATRM00000...	Lightning Perf...	December 01,...	13	0	Daily	

For more information on Event Log Files, see [Using Event Monitoring](#).

Configure Remote Site Settings

Configure settings for a remote site.

Before any Visualforce page, Apex callout, or JavaScript code using XMLHttpRequest in an s-control or custom button can call an external site, that site must be registered in the Remote Site Settings page, or the call fails.

To access the page, from Setup, enter *Remote Site Settings* in the Quick Find box, then select **Remote Site Settings**. This page displays a list of any remote sites already registered and provides additional information about each site, including remote site name and URL.

For security reasons, Salesforce restricts the outbound ports you can specify to one of the following:

- 80: This port only accepts HTTP connections.
- 443: This port only accepts HTTPS connections.
- 1024–65535 (inclusive): These ports accept HTTP or HTTPS connections.

To register a new site:

1. Click **New Remote Site**.
2. Enter a descriptive term for the `Remote Site Name`.
3. Enter the URL for the remote site.
4. To allow access to the remote site regardless of whether the user's connection is over HTTP or HTTPS, select the `Disable Protocol Security` checkbox. When selected, Salesforce can pass data from an HTTPS session to an HTTP session, and vice versa. Only select this checkbox if you understand the security implications.
5. Optionally, enter a description of the site.
6. Click **Save** to finish, or click **Save & New** to save your work and begin registering an additional site.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

Visualforce and S-controls aren't available in **Database.com**

USER PERMISSIONS

To configure remote settings:

- **Customize Application or Modify All Data**

 **Tip:** For best performance, verify that your remote HTTPS encrypted sites have OSCP (Online Certificate Status Protocol) stapling turned on.

SEE ALSO:

[Manage Trusted URLs](#)

Named Credentials

A named credential specifies the URL of a callout endpoint and its required authentication parameters in one definition. To simplify the setup of authenticated callouts, specify a named credential as the callout endpoint.

 **Important:** In Winter '23, Salesforce introduced an improved named credential that is extensible and customizable. We strongly recommend that you use this preferred credential instead of legacy named credentials. For information on extensible, customizable named credentials, see [Named Credentials and External Credentials](#). Legacy named credentials are deprecated and will be discontinued in a future release.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **All Editions**

Salesforce manages all authentication for callouts that specify a named credential as the callout endpoint. You can also skip remote site settings, which are otherwise required for callouts to external sites, for the site defined in the named credential.

 **Note:** All credentials stored by this feature set are encrypted under a framework that's consistent with other encryption frameworks on the platform. Salesforce encrypts your credentials by auto-creating org-specific keys.

Named credentials are supported in these types of callout definitions.

- Apex callouts
- External data sources
- External Services

By separating the endpoint URL and authentication from the callout definition, named credentials make callouts easy to maintain. For example, if an endpoint URL changes, you update only the named credential. All callouts that reference the named credential continue to work.

If you have multiple orgs, you can create a named credential with the same name but with a different endpoint URL in each org. You can then package and deploy one callout definition on all the orgs that references the shared name of those named credentials. For example, the named credential in each org can have a different endpoint URL to accommodate differences in development and production environments. If an Apex callout specifies the shared name of those named credentials, the Apex class that defines the callout can be packaged and deployed on all those orgs without programmatically checking the environment.

A named credential supports various authentication protocols. You can set up each named credential to use an org-wide named principal or per-user authentication. A named principal applies the same credential or authentication configuration for the entire org, while per-user authentication provides access control at the individual user level.

You can append a query string to a named credential URL. Use a question mark (?) as the separator between the named credential URL and the query string. For example:

```
callout:My_Named_Credential/some_path?format=json
```

 **Note:** If you're transmitting sensitive information such as healthcare data or credit card data, use authenticated named credentials. We recommend that customers provide their own certificates for extra security of sensitive data transmissions.

Named Credentials and External Credentials

To simplify the setup of authenticated callouts, specify a named credential as the callout endpoint. Create an external credential to specify an authentication protocol and permission set or profile to use when authenticating to an external system. Add custom headers to named and external credentials to cover more use cases and security requirements. You can create and configure named credentials programmatically or through the Salesforce app UI.

Legacy Named Credentials

A legacy named credential specifies the URL of a callout endpoint and its required authentication parameters in one definition. Legacy named credentials are deprecated and are unsupported in future releases.

Authentication Protocols for Named Credentials

Your connections between Salesforce and external systems use an authentication protocol to confirm secure communication between the two systems. Choose the authentication protocol that matches the configuration of the external system that you connect to. When you do, keep the strengths and considerations of each authentication protocol in mind.

Set Up JWT Claims for Named Credentials

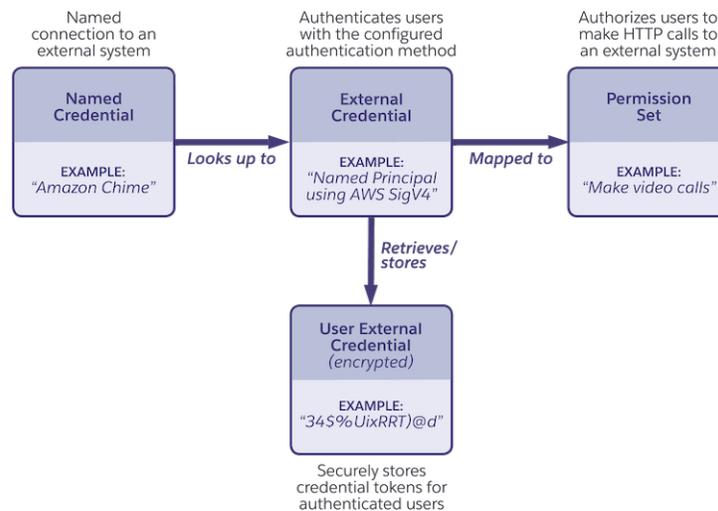
External credentials that use JWT authentication have JWT (JSON Web Token) claims. JWT claims assert attributes about tokens, such as time of expiration. You can modify some default claims for an external credential as well as create your own custom claims.

Named Credentials and External Credentials

To simplify the setup of authenticated callouts, specify a named credential as the callout endpoint. Create an external credential to specify an authentication protocol and permission set or profile to use when authenticating to an external system. Add custom headers to named and external credentials to cover more use cases and security requirements. You can create and configure named credentials programmatically or through the Salesforce app UI.

EDITIONS

Available in: All Editions



Parts of the Named Credential Schema

Named credentials and external credentials simplify and enable greater reuse of setup for secure and authenticated callouts.

- A named credential specifies a callout endpoint and an HTTP transport protocol.
- An external credential's authentication protocol and user credentials authenticate the caller. More than one named credential can use the same external credential.

- External credential principals map to user permissions to authorize them to make callouts.
- User external credentials store encrypted tokens.

Named Credentials

A named credential is a logical entity that can be thought of as a named connection to an external system. With named credentials, there's no need to embed a physical URL into Apex code and manage authentication tokens in unencrypted data stores. Instead, a variable in the code allows an administrator to provision the physical endpoint at deployment time and manage user credentials in the organization's encrypted credential store. The named credential URL is resolved at runtime to the configured physical endpoint along with the credentials for the authorized user performing the callout.

Named credentials support different types, with a default of Secure Endpoint. Advanced use cases can benefit from storing custom parameters, which are also supported. A parameter is essentially a name-value pair to capture arbitrary metadata, and the parameter values are stored securely. See the API documentation for more details.

The named credential *type* can be one of the following.

- SecuredEndpoint—The named credential includes an endpoint's transport protocol as secured through transport layer security (TLS).
- PrivateEndpoint—The named credential sends traffic through a private connection, bypassing the public internet.
- Legacy—A legacy named credential specifies the URL of a callout endpoint and its required authentication parameters in one definition.

 **Important:** Legacy named credentials are deprecated and will be discontinued in a future release.

A named credential can be customized. For example, you can define HTTP headers with Salesforce formula functions to tailor header values to the calling user context or substitute formula function variables in the request body.

External Credentials

Security policies often mandate that authentication details change on a rotating basis. An external credential encapsulates the details of how Salesforce authenticates to a remote system. By externalizing authentication information from the code, developers aren't required to change these details to stay compliant with such policies.

Hyperscale cloud infrastructure providers often host many different systems, and a single set of credentials can be used to access multiple named systems. A named credential holds a reference to an external credential, and multiple named credentials can benefit from sharing a single external credential. For example, a Salesforce integration can access the APIs for Google Drive and Google Calendar with the same credentials.

Authentication protocols such as OAuth or AWS Signature v4 specify how to authenticate with an external system. For example, they can specify how access keys are exchanged or how to refresh expired access keys. The protocol specifies implementation details handled by the platform, such as how keys are exchanged and when they're refreshed. Authentication parameters are captured as external credential name-value pairs. See the API documentation for authentication of protocol-specific parameters.

Permission Sets, External Credentials, and User External Credentials

The Salesforce platform supports the use of permission sets to control which users are authorized to make callouts. External credentials authenticate users, and permission sets authorize users. You link an external credential to permission sets or user profiles through principals and at run time, the platform ensures that the user has the permission set before accessing the remote system. Development teams can choose to package permission sets representing access to a specific remote system, though administrators retain the option to associate the external credential with other permission sets of their choosing. To reduce the effort to grant credential permissions to a large number of users, you can link permission sets to permission set groups.

 **Tip:** To apply credential permissions to the largest number of users, link a permission set to a principal and add the permission set to a permission set group.

Tokens are encrypted and stored in a user external credential object. Any user performing an authenticated callout needs profile- or permission set-based access to user external credentials.

Custom Headers

Custom headers are a way for a remote system to define parameters it needs as input to respond to a request. See [Custom Headers for Credentials](#).

Creating and Editing Credentials

We recommend creating named and external credentials through the Salesforce UI. You can also create credentials through the Metadata, Tooling, and Connect REST APIs.

[Create and Edit an External Credential](#)

An external credential represents the details of how Salesforce authenticates to an external system via an authentication protocol. It also links to permission sets and profiles, and, optionally, custom headers.

[User External Credentials](#)

User external credential objects store encrypted tokens used by named credentials. You must enable user external credentials to use named credentials.

[Custom Headers for Credentials](#)

You can add custom headers to named credentials and external credentials. Custom headers are a way for a remote system to define parameters it needs as input to respond to a request. Using a custom header is similar to having a function in a piece of code and defining input parameters or arguments that allow the caller to provide input.

[Create and Edit a Named Credential](#)

A named credential specifies the URL of a callout endpoint and its required authentication parameters in one definition. A named credential can be specified as an endpoint to simplify the setup of authenticated callouts. Named credentials connect to external credentials.

SEE ALSO:

[Connect REST API Developer Guide: Named Credentials Resources](#)

[Apex Reference Guide: NamedCredentials Class](#)

[Apex Developer Guide: Invoking Callouts Using Apex](#)

Create and Edit an External Credential

An external credential represents the details of how Salesforce authenticates to an external system via an authentication protocol. It also links to permission sets and profiles, and, optionally, custom headers.

Before creating a named credential, you must create at least one external credential to map the named credential to.

Here are the overall steps for using external credentials. The specific steps vary depending on the authentication protocol you choose. For more on authentication protocols, see [Authentication Protocols for Named Credentials](#).

1. Give the external credential a name and label, and choose an authentication protocol.
2. Create principals that map to permission sets, permission set groups, or profiles.
3. Optionally, create a custom header for the external credential.
4. Authorize user external credentials. Authorize one time for each permission set or user.
5. In a named credential, link to the external credential you created.

[Create and Edit an OAuth External Credential](#)

External credentials support four different variants of the OAuth authentication protocol.

[Create and Edit an AWS Signature v4 External Credential](#)

Follow these steps for creating an external credential if you're using AWS Signature v4 authentication.

[Create and Edit a Custom Authentication External Credential](#)

Follow these steps for creating an external credential if you're using a custom authentication.

[Create and Edit a No Authentication External Credential](#)

Follow these steps for creating an external credential if you're using no authentication.

[Create and Edit a JWT External Credential](#)

Follow these steps for creating an external credential if you're using JWT authentication.

[Create and Edit a Basic Authentication External Credential](#)

Follow these steps to create an external credential if you're using Basic authentication.

[Additional Tasks for External Credentials](#)

After you created an external credential, there are a few more things to do to make the credential useful.

[Enable External Credential Principals](#)

To make callouts that use a named credential, you must enable principal access to permission sets or profiles for the users who need access.

Create and Edit an OAuth External Credential

External credentials support four different variants of the OAuth authentication protocol.

[Create and Edit an OAuth External Credential with the Browser Flow](#)

Follow these steps for creating an external credential if you're using OAuth authentication with the Browser Flow.

[Create and Edit an OAuth External Credential with the JWT Bearer Flow](#)

Follow these steps for creating an external credential if you're using OAuth authentication with the JWT Bearer Flow.

EDITIONS

Available in: **All** Editions.

USER PERMISSIONS

To view external credentials:

- View Setup and Configuration

To create, edit, or delete external credentials:

- Manage Named Credentials or Customize Applications

[Create and Edit an OAuth External Credential with the Client Credentials with JWT Assertion Flow](#)

Follow these steps for creating an external credential if you're using OAuth authentication with the Client Credentials with JWT Assertion Flow.

[Create and Edit an OAuth External Credential with the Client Credentials with Client Secret Flow](#)

Follow these steps to create an external credential if you're using OAuth authentication with the Client Credentials with Client Secret Flow. Use the Client Credentials with Client Secret flow when Salesforce is a client application of another external system that has its own login credentials. Rather than managing access to the external system on a per-user basis, you can set up service-level access for your Salesforce org. Then, use Salesforce user profiles or permission sets to grant access to users who perform authenticated callouts.

Create and Edit an OAuth External Credential with the Browser Flow

Follow these steps for creating an external credential if you're using OAuth authentication with the Browser Flow.

1. From Setup, in the Quick Find box, enter *Named Credentials*, and then select **Named Credentials**.
2. Click **External Credentials**.
3. To create a new external credential, click **New**. To edit an existing external credential, click its link in the list of external credentials and then click **Edit**.
4. Complete the fields.

Field	Description
Label	A user-friendly name for the external credential that's displayed in the Salesforce user interface, such as in list views.
Name	A unique identifier that's used to refer to this external credential from callout definitions and through the API. The name can contain only underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.
Authentication Protocol	Select OAuth 2.0 .
Authentication Flow Type	Select Browser Flow . For information on the OAuth 2.0 variants, see Authentication Protocols for Named Credentials .
Scope	Optional. Specifies the scope of permissions to request for the access token. A scope declared here is a credential-level scope that applies to all callouts that use this credential. Your authentication provider determines the allowed values. See OAuth Tokens and Scopes and Use the Scope Parameter . The Scope field accepts static values and formulas. For instance, use a static scope value that specifies that all callouts using this credential request have offline access. Or enter a formula to request access

EDITIONS

Available in: All Editions

USER PERMISSIONS

To view external credentials:

- View Setup and Configuration

To create, edit, or delete external credentials:

- Manage Named Credentials or Customize Applications

Field	Description
	<p>dynamically. This example uses the <code>session:role</code> scope to request credential-level access based on each user's department.</p> <pre>{!"session:role:" + \$User.Department}</pre> <p>When you create an external credential's principal, you can also specify principal-level scopes, which apply only per principal. For example, create a principal-level scope to request access only for users that work in the Administration or Management departments.</p> <p>When you set the credential's scope, keep these considerations in mind.</p> <ul style="list-style-type: none"> • The value that you enter replaces the <code>Default Scopes</code> value that's defined in the specified authentication provider. • A scope can affect whether each OAuth flow prompts the user with a consent screen. • We recommend that you request a refresh token or offline access. Otherwise, when the token expires, you lose access to the external system.
Authentication Provider	Specify the Authentication Provider . See Authentication Providers .

5. Save the external credential.

Create Principals

After you create an external credential that uses OAuth authentication with the Browser Flow, create principals for it. You link an external credential to permission sets or user profiles through principals, and at run time, the platform ensures that the user has the permission set before accessing the remote system.

1. On the Named Credentials page, click **External Credential**.
2. Select the external credential that you created.
3. Scroll to Principals.
4. To create a principal for the external credential, click **New** or select **Edit** from the Actions menu of an existing principal.
When editing an existing principal, not all the fields listed here are modifiable.
5. Enter the information for the principal.

Field	Description
Parameter Name	Enter a name for the principal, such as <i>Admin</i> or <i>Marketing Group</i> .
Sequence Number	Assign a sequence number. A sequence number specifies the order of principals to apply when a user participates in more than one principal. For example, a user could be part of multiple permission sets that are applicable for a credential provider. Priority is from lower to higher numbers.
Identity Type	<p>Choose either Named Principal or Per-User Principal.</p> <p>You can set up each external credential to use an org-wide named principal or per-user authentication. A named principal applies the same credential or authentication configuration for the entire org, while per-user authentication provides access control at the individual user level.</p>

Field	Description
Scope	<p>Optional. Enter a principal-level scope.</p> <p>This scope is in addition to the optional credential-level scope. You can use it to provide access parameters on a per-principal basis. For example, the credential-level scope can specify offline token access, while the principal-level scope can specify access for users with certain roles, such as Marketing or System Administrator.</p> <p>Credential-level and principal-level scopes are concatenated together in callouts and sent as a space-separated list. These scopes overwrite an authentication provider's default scopes, if the appended list is non-null.</p> <p>This example uses a principal-level scope to link a group of authenticated users to roles on an external site. The scope is <code>session:role:<role></code>. If a user has Sales or Service in their department name, the scope is set as <code>session:role:Sales</code> or <code>session:role:Service</code>.</p> <pre>{!IF(OR(CONTAINS(\$User.Department, "Sales"), CONTAINS(\$User.Department, "Service")), "session:role:" + \$User.Department, "")}</pre>

6. Save the principal.
You can't modify the Principal Name and Identity Type of an existing principal. To change these parameters, delete the principal and recreate it.
7. Map the principal to a permission set or profile. See [Enable External Credential Principals](#). You can map a principal to multiple permission sets, permission set groups, or profiles.
8. To authorize the external credential when the principal's Identity Type is set to Named Principal, select **Authenticate** from the principal's Actions menu. Then, authenticate yourself to the system. For example, enter a username and password.
9. To authorize the external credential when the principal's Identity Type is set to Per-User Principal:
 - a. From your personal settings, in the Quick Find box, enter *External Credentials*, and then select **External Credentials**.
 - b. In the tile of the external credential that you want to authenticate, click **Allow Access**.
 - c. Authenticate yourself to the external system. For example, enter a username and password.

The external credential is authenticated, and its tile shows Configured. To revoke authentication on an external credential, click **Revoke Access**.

Now that you created the external credential and mapped its principal to a permission set or profile, it's time to:

- Enable the user external credentials that Salesforce created automatically when you saved the principal. User external credentials store the encrypted authentication tokens used by named credentials, and you grant access so that users can access the tokens when they perform authenticated callouts. See [Enable User External Credentials](#).
- Create the connected name credential. See [Create and Edit a Named Credential](#).
- Add optional custom headers to named credentials and external credentials. See [Custom Headers for Credentials](#).

SEE ALSO:

[OAuth 2.0 Client Credentials Flow for Server-to-Server Integration](#)

Create and Edit an OAuth External Credential with the JWT Bearer Flow

Follow these steps for creating an external credential if you're using OAuth authentication with the JWT Bearer Flow.

1. From Setup, in the Quick Find box, enter *Named Credentials*, and then select **Named Credentials**.
2. Click **External Credentials**.
3. To create a new external credential, click **New**. To edit an existing external credential, click its link in the list of external credentials and then click **Edit**.
4. Complete the fields.

Field	Description
Label	A user-friendly name for the external credential that's displayed in the Salesforce user interface, such as in list views.
Name	<p>A unique identifier that's used to refer to this external credential from callout definitions and through the API.</p> <p>The name can contain only underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.</p>
Authentication Protocol	Select OAuth 2.0 .
Authentication Flow Type	Select JWT Bearer Flow . For information on the OAuth 2.0 variants, see Authentication Protocols for Named Credentials .
Scope	<p>Optional. Specifies the scope of permissions to request for the access token. A scope declared here is a credential-level scope that applies to all callouts that use this credential. Your authentication provider determines the allowed values. See OAuth Tokens and Scopes and Use the Scope Parameter.</p> <p>The Scope field accepts static values and formulas. For instance, use a static scope value that specifies that all callouts using this credential request have offline access. Or enter a formula to request access dynamically. This example uses the <code>session:role</code> scope to request credential-level access based on each user's department.</p> <pre>{!"session:role:" + \$User.Department}</pre> <p>When you create an external credential's principal, you can also specify principal-level scopes, which apply only per principal. For example, create a principal-level scope to request access only for users that work in the Administration or Management departments.</p> <p>When you set the credential's scope, keep these considerations in mind.</p> <ul style="list-style-type: none"> • The value that you enter replaces the <code>Default Scopes</code> value that's defined in the specified authentication provider.

EDITIONS

Available in: All Editions

USER PERMISSIONS

To view external credentials:

- View Setup and Configuration

To create, edit, or delete external credentials:

- Manage Named Credentials or Customize Applications

Field	Description
	<ul style="list-style-type: none"> • A scope can affect whether each OAuth flow prompts the user with a consent screen. • We recommend that you request a refresh token or offline access. Otherwise, when the token expires, you lose access to the external system.
Identity Provider URL	The URL of the identity provider to send the JWT (JSON Web Token) to in exchange for an access token.
Signing Certificate	A certificate from an identity provider, via a CA (certificate authority), or registered with an identity provider, and uploaded to Salesforce through Certificate and Key Management.
Signing Algorithm	Select from RS256 (default) or RS512.

For common claims, see [Set Up JWT Claims for Named Credentials](#).

5. Save the external credential.

Create Principals

After you create an external credential that uses OAuth authentication with the JWT Bearer Flow, create principals for it. You link an external credential to permission sets or user profiles through principals, and at run time, the platform ensures that the user has the permission set before accessing the remote system.

1. On the Named Credentials page, click **External Credential**.
2. Select the external credential that you created.
3. Scroll to Principals.
4. To create a principal for the external credential, click **New** or select **Edit** from the Actions menu of an existing principal.
When editing an existing principal, not all the fields listed here are modifiable.
5. Enter the information for the principal.

Field	Description
Parameter Name	Enter a name for the principal, such as <i>Admin</i> or <i>Marketing Group</i> .
Sequence Number	Assign a sequence number. A sequence number specifies the order of principals to apply when a user participates in more than one principal. For example, a user could be part of multiple permission sets that are applicable for a credential provider. Priority is from lower to higher numbers.
Identity Type	Choose either Named Principal or Per-User Principal . You can set up each external credential to use an org-wide named principal or per-user authentication. A named principal applies the same credential or authentication configuration for the entire org, while per-user authentication provides access control at the individual user level.
Scope	Optional. Enter a principal-level scope. This scope is in addition to the optional credential-level scope. You can use it to provide access parameters on a per-principal basis. For example, the credential-level scope can specify offline

Field	Description
	<p>token access, while the principal-level scope can specify access for users with certain roles, such as Marketing or System Administrator.</p> <p>Credential-level and principal-level scopes are concatenated together in callouts and sent as a space-separated list. These scopes overwrite an authentication provider's default scopes, if the appended list is non-null.</p> <p>This example uses a principal-level scope to link a group of authenticated users to roles on an external site. The scope is <code>session:role:<role></code>. If a user has Sales or Service in their department name, the scope is set as <code>session:role:Sales</code> or <code>session:role:Service</code>.</p> <pre data-bbox="527 604 1445 709"> {! IF (OR (CONTAINS (\$User.Department, "Sales"), CONTAINS (\$User.Department, "Service")), "session:role:" + \$User.Department, "") } </pre>

6. Save the principal.
You can't modify the Principal Name and Identity Type of an existing principal. To change these parameters, delete the principal and recreate it.
7. Map the principal to a permission set or profile. See [Enable External Credential Principals](#). You can map a principal to multiple permission sets, permission set groups, or profiles.

Now that you created the external credential and mapped its principal to a permission set or profile, it's time to:

- Enable the user external credentials that Salesforce created automatically when you saved the principal. User external credentials store the encrypted authentication tokens used by named credentials, and you grant access so that users can access the tokens when they perform authenticated callouts. See [Enable User External Credentials](#).
- Create the connected name credential. See [Create and Edit a Named Credential](#).
- Add optional custom headers to named credentials and external credentials. See [Custom Headers for Credentials](#).

SEE ALSO:

[OAuth 2.0 Client Credentials Flow for Server-to-Server Integration](#)

Create and Edit an OAuth External Credential with the Client Credentials with JWT Assertion Flow

Follow these steps for creating an external credential if you're using OAuth authentication with the Client Credentials with JWT Assertion Flow.

1. From Setup, in the Quick Find box, enter *Named Credentials*, and then select **Named Credentials**.
2. Click **External Credentials**.
3. To create a new external credential, click **New**. To edit an existing external credential, click its link in the list of external credentials and then click **Edit**.
4. Complete the fields.

Field	Description
Label	A user-friendly name for the external credential that's displayed in the Salesforce user interface, such as in list views.
Name	<p>A unique identifier that's used to refer to this external credential from callout definitions and through the API.</p> <p>The name can contain only underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.</p>
Authentication Protocol	Select OAuth 2.0 .
Authentication Flow Type	Select Client Credentials with JWT Assertion Flow . For information on the OAuth 2.0 variants, see Authentication Protocols for Named Credentials .
Scope	<p>Optional. Specifies the scope of permissions to request for the access token. This scope applies to all callouts that use this credential. Your authentication provider determines the allowed values. See OAuth Tokens and Scopes and Use the Scope Parameter.</p> <p>For instance, you can create a scope to specify that all callouts using this credential request have offline access.</p> <p>The Scope field accepts static values and formulas. For instance, use a static scope value that specifies that all callouts using this credential request have offline access. Or enter a formula to request access dynamically. This example uses the <code>session:role</code> scope to request access based on each user's department.</p> <pre>{!"session:role:" + \$User.Department }</pre> <ul style="list-style-type: none"> • The value that you enter replaces the <code>Default Scopes</code> value that's defined in the specified authentication provider. • A scope can affect whether each OAuth flow prompts the user with a consent screen.

EDITIONS

Available in: All Editions

USER PERMISSIONS

To view external credentials:

- View Setup and Configuration

To create, edit, or delete external credentials:

- Manage Named Credentials or Customize Applications

Field	Description
	<ul style="list-style-type: none"> We recommend that you request a refresh token or offline access. Otherwise, when the token expires, you lose access to the external system.
Identity Provider URL	The URL of the identity provider to send the JWT (JSON Web Token) to in exchange for an access token.
Signing Certificate	A certificate from an identity provider, via a CA (certificate authority), or registered with an identity provider, and uploaded to Salesforce through Certificate and Key Management.
Signing Algorithm	Select from RS256 (default) or RS512.

For common claims, see [Set Up JWT Claims for Named Credentials](#).

5. Save the external credential.

Create Principals

After you create an external credential that uses the OAuth 2.0 Client Credentials with JWT Assertion Flow, create principals for it. You link an external credential to permission sets or user profiles through principals, and at run time, the platform ensures that the user has the permission set before accessing the remote system.

Principals that authenticate with JWT use the Named Principal identity type automatically because the authentication configuration is applied at the service level.

1. On the Named Credentials page, click **External Credential**.
2. Select the external credential that you created.
3. Scroll to Principals.
4. To create a principal for the external credential, click **New** or select **Edit** from the Actions menu of an existing principal.
When editing an existing principal, not all the fields listed here are modifiable.
5. Enter the information for the principal.

Field	Description
Parameter Name	Enter a name for the principal, such as <i>Admin</i> or <i>Marketing Group</i> .
Sequence Number	Assign a sequence number. A sequence number specifies the order of principals to apply when a user participates in more than one principal. For example, a user could be part of multiple permission sets that are applicable for a credential provider. Priority is from lower to higher numbers.
Client ID	Enter the unique identifier that is used to authenticate the client.

6. Save the principal.
You can't modify the Principal Name and Identity Type of an existing principal. To change these parameters, delete the principal and recreate it.
7. Map the principal to a permission set or profile. See [Enable External Credential Principals](#). You can map a principal to multiple permission sets, permission set groups, or profiles.

Now that you created the external credential and mapped its principal to a permission set or profile, it's time to:

- Enable the user external credentials that Salesforce created automatically when you saved the principal. User external credentials store the encrypted authentication tokens used by named credentials, and you grant access so that users can access the tokens when they perform authenticated callouts. See [Enable User External Credentials](#).
- Create the connected name credential. See [Create and Edit a Named Credential](#).
- Add optional custom headers to named credentials and external credentials. See [Custom Headers for Credentials](#).

SEE ALSO:

[OAuth 2.0 Client Credentials Flow for Server-to-Server Integration](#)

Create and Edit an OAuth External Credential with the Client Credentials with Client Secret Flow

Follow these steps to create an external credential if you're using OAuth authentication with the Client Credentials with Client Secret Flow. Use the Client Credentials with Client Secret flow when Salesforce is a client application of another external system that has its own login credentials. Rather than managing access to the external system on a per-user basis, you can set up service-level access for your Salesforce org. Then, use Salesforce user profiles or permission sets to grant access to users who perform authenticated callouts.

Before you create an OAuth 2.0 external credential in Salesforce, register Salesforce as a client application in an external system. Generate and save the client credentials—client ID and client secret—on your local machine. You need the copied values when you set up the external credential and principal in Salesforce.

1. From Setup, in the Quick Find box, enter *Named Credentials*, and then select **Named Credentials**.
2. Click **External Credentials**.
3. To create a new external credential, click **New**. To edit an existing external credential, click its link in the list of external credentials, and then click **Edit**.
4. Complete the fields.

EDITIONS

Available in: All Editions

USER PERMISSIONS

To view external credentials:

- View Setup and Configuration

To create, edit, or delete external credentials:

- Manage Named Credentials or Customize Applications

Field	Description
Label	A user-friendly name for the external credential that's displayed in the Salesforce user interface, such as in list views.
Name	A unique identifier that's used to refer to this external credential from callout definitions and through the API. The name can contain only underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.
Authentication Protocol	Select OAuth 2.0 .
Authentication Flow Type	Select Client Credentials with Client Secret Flow . For information on the OAuth 2.0 variants, see Authentication Protocols for Named Credentials .

Field	Description
Scope	<p>Optional. Specifies the scope of permissions to request for the access token. This scope applies to all callouts that use this credential. Your authentication provider determines the allowed values. See OAuth Tokens and Scopes and Use the Scope Parameter.</p> <p>The Scope field accepts static values and formulas. For instance, use a static scope value that specifies that all callouts using this credential request have offline access. Or enter a formula to request access dynamically. This example uses the <code>session:role</code> scope to request access based on each user's department.</p> <pre>{!"session:role:" + \$User.Department}</pre> <p>When you set the credential's scope, keep these considerations in mind.</p> <ul style="list-style-type: none"> • The value that you enter replaces the <code>Default Scopes</code> value that's defined in the specified authentication provider. • A scope can affect whether each OAuth flow prompts the user with a consent screen. • We recommend that you request a refresh token or offline access. Otherwise, when the token expires, you lose access to the external system.
Identity Provider URL	The URL of the identity provider to send the client credentials to in exchange for an access token.
Pass client credentials in request body	<p>Optional. Sends the client ID and client secret in the callout's request body instead of its header. By default, client credentials are sent in the callout's authorization header, as with Basic authentication. With this format, the <code>client_id</code> is appended to the <code>client_secret</code> in the format <code>client_id:client_secret</code>, and the resulting value is Base64-encoded.</p> <p>Sending client credentials in the authorization header aligns with section 2.3.1 Client Password in The OAuth 2.0 Authorization Framework from the Internet Engineering Task Force. If the external system requires that you pass client credentials in the request body instead, use this option.</p>

5. Save the external credential.

Create Principals

After you create an external credential that uses the OAuth Client Credentials with Client Secret Flow, create principals for it. You link an external credential to permission sets or user profiles through principals, and at run time, the platform ensures that the user has the permission set before accessing the remote system.

Principals that authenticate with Client Credentials with Client Secret use the Named Principal identity type automatically because the authentication configuration is applied at the service level.

1. On the Named Credentials page, click **External Credential**.
2. Select the external credential that you created.
3. Scroll to Principals.
4. To create a principal for the external credential, click **New** or select **Edit** from the Actions menu of an existing principal. When editing an existing principal, not all the fields listed here are modifiable.
5. Enter the information for the principal.

Field	Description
Parameter Name	Enter a name for the principal, such as <i>Admin</i> or <i>Marketing Group</i> .
Sequence Number	Assign a sequence number. A sequence number specifies the order of principals to apply when a user participates in more than one principal. For example, a user could be part of multiple permission sets that are applicable for a credential provider. Priority is from lower to higher numbers.
Client ID	Enter the unique identifier that is used to authenticate the client.
Client Secret	Enter the secret for your client.

 **Tip:** Client secrets often contain special characters. If your client ID or client secret contains special characters, you must URL-encode it before you save it in your principal.

- Save the principal.
You can't modify the Principal Name and Identity Type of an existing principal. To change these parameters, delete the principal and recreate it.
- Map the principal to a permission set or profile. See [Enable External Credential Principals](#). You can map a principal to multiple permission sets, permission set groups, or profiles.

Now that you created the external credential and mapped its principal to a permission set or profile, it's time to:

- Enable the user external credentials that Salesforce created automatically when you saved the principal. User external credentials store the encrypted authentication tokens used by named credentials, and you grant access so that users can access the tokens when they perform authenticated callouts. See [Enable User External Credentials](#).
- Create the connected name credential. See [Create and Edit a Named Credential](#).
- Add optional custom headers to named credentials and external credentials. See [Custom Headers for Credentials](#).

SEE ALSO:

[OAuth 2.0 Client Credentials Flow for Server-to-Server Integration](#)

Create and Edit an AWS Signature v4 External Credential

Follow these steps for creating an external credential if you're using AWS Signature v4 authentication.

Named credentials support two variants of the AWS Signature v4 authentication protocol: IAM User Identified by Access Key and Roles Anywhere.

- From Setup, in the Quick Find box, enter *Named Credentials*, and then select **Named Credentials**.
- Click **External Credentials**.
- To create a new external credential, click **New**. To edit an existing external credential, click its link in the list of external credentials and then click **Edit**.
- Complete the fields.

EDITIONS

Available in: **All Editions**

USER PERMISSIONS

To view external credentials:

- View Setup and Configuration

To create, edit, or delete external credentials:

- Manage Named Credentials or Customize Applications

Field	Description
Label	A user-friendly name for the external credential that's displayed in the Salesforce user interface, such as in list views.
Name	<p>A unique identifier that's used to refer to this external credential from callout definitions and through the API.</p> <p>The name can contain only underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.</p>
Authentication Protocol	Choose AWS Signature 4 .
Service	The name of an AWS service, such as dynamodb or athena.
Region	An AWS geographic region, such as us-west-1 (United States West).
AWS Account ID	Optional. The 12-digit number that uniquely identifies your AWS account.
Obtain Temporary IAM Credentials via STS	<p>Optional. If you want to use STS, pick one of using these credential types:</p> <ul style="list-style-type: none"> • IAM User Identified by Access Key • Roles Anywhere (Assume an IAM Role via Certificate) <p>See Authentication Protocols for Named Credentials for information on these variants.</p> <p>If you're using Amazon API Gateway, configure the Gateway Response for Expired Token so that it returns a 400 or 401 HTTP code. Salesforce then can refresh the token when it expires. A 403 code doesn't cause a token refresh because it's reserved for scenarios where the token is valid but the caller doesn't have access to the resource.</p>

5. If you selected **Obtain Temporary IAM Credentials via STS**, complete fields for the corresponding credential type.
- a. For the IAM User Identified by Access Key credential type:

Field	Description
STS Access Key	The access key ID for the AWS access key.
STS Access Secret	The access secret for the AWS access key.
STS External ID	<p>The AWS <code>ExternalId</code> value that can be used when delegating account access to a third party. This value helps ensure that only a specified third party can access the role.</p> <p>Using an External ID such as</p> <pre>salesforceIntegration-<i>unique_phrase</i></pre> <p>For example</p> <pre>salesforceIntegration-abc123</pre> <p>ensures that the server side can identify Salesforce as the client assuming the IAM Role.</p>

Field	Description
STS Duration	Optional. Numeric value in seconds, for example, 3600. Maximum value: 43200 (12 hours).

- b. For the Roles Anywhere credential type:

Field	Description
Trust Anchor ARN	The Amazon Resource Name for the trust anchor. A trust anchor is either a reference to AWS Private Certificate Authority (AWS Private CA) or another CA certificate.
Profile ARN	The Amazon Resource Name for the Amazon profile. Profiles are predefined sets of permissions that are applied after successfully authenticating with Roles Anywhere. Profiles map to one or more IAM roles.
Signing Certificate	A certificate from AWS, via a CA (certificate authority), and uploaded to Salesforce through Certificate and Key Management.
STS Duration	Optional. Numeric value in seconds, for example, 3600. Maximum value: 43200 (12 hours).

6. Save the external credential. You're taken to the Named Credentials screen.

Create Principals for AWS Signature v4

After you've created an external credential that uses AWS Signature v4 authentication, create principals for it. These principals get mapped to permission sets and profiles.

1. On the Named Credentials page, click **External Credential**.
2. Select the external credential you created.
3. Scroll to Principals.
4. Click **New** to create a principal for this external credential, or choose **Edit** from the Actions menu of an existing principal. When editing an existing principal, not all the fields listed here are modifiable.
5. Complete the following fields. If you're using STS, the Access Key and Secret fields are disabled and display the temporary credentials, if any.

Field	Description
Parameter Name	Enter a name for the principal, such as <i>Admin</i> or <i>Marketing Group</i> .
Sequence Number	Assign a sequence number. A sequence number specifies the order of principals to apply when a user participates in more than one principal. For example, a user could be part of multiple permission sets that are applicable for a credential provider. Priority is from lower to higher numbers.

Field	Description
Access Key	Optional. The access key ID for the AWS access key.
Access Secret	Optional. The access secret for the AWS access key.
IAM Role ARN	Optional. The Amazon Resource Name (ARN) of the role that the credential assumes.

- Save the principal.
You can't modify the Principal Name and Identity Type of an existing principal. To change these parameters, delete the principal and recreate it.
- Map the principal to a permission set or profile. See [Enable External Credential Principals](#). You can map a principal to multiple permission sets, permission set groups, or profiles.

Congratulations—you've finished the main steps in creating an AWS Signature v4 external credential. See [Additional Tasks for External Credentials](#) for a few more jobs to complete.

Create and Edit a Custom Authentication External Credential

Follow these steps for creating an external credential if you're using a custom authentication.

If you choose Custom as your authentication protocol, you must specify a principal, sequence number, and authentication parameters. Each authentication parameter requires a name and value. Authentication parameters can be used in custom headers as a formula, for example, `$(Credential.EC_dev_name.AuthParam_name)`. See [Custom Headers for Credentials](#), [Create and Edit Custom Headers](#), and [Using Basic Authentication with Named Credentials](#).

- From Setup, enter *Named Credentials* in the Quick Find box, then select **Named Credentials**.
- Click **External Credentials**.
- To create a new external credential, click **New**. To edit an existing external credential, click its link in the list of external credentials and then click **Edit**.
- Complete the fields.

Field	Description
Label	A user-friendly name for the external credential that's displayed in the Salesforce user interface, such as in list views.
Name	A unique identifier that's used to refer to this external credential from callout definitions and through the API. The name can contain only underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.
Authentication Protocol	Select Custom .

- Save the external credential. You're taken to the Named Credentials screen.

EDITIONS

Available in: **All Editions**.

USER PERMISSIONS

To view external credentials:

- View Setup and Configuration

To create, edit, or delete external credentials:

- Manage Named Credentials or Customize Applications

Create Principals for Custom Authentication

After you've created an external credential that uses custom authentication, create principals for it. These principals get mapped to permission sets and profiles.

1. On the Named Credentials page, click **External Credential**.
2. Select the external credential you created.
3. Scroll to Principals.
4. Click **New** to create a principal for this external credential, or choose **Edit** from the Actions menu of an existing principal. When editing an existing principal, not all the fields listed here are modifiable.
5. Complete the following fields.

Field	Description
Parameter Name	Enter a name for the principal, such as <i>Admin</i> or <i>Marketing Group</i> .
Sequence Number	Assign a sequence number. A sequence number specifies the order of principals to apply when a user participates in more than one principal. For example, a user could be part of multiple permission sets that are applicable for a credential provider. Priority is from lower to higher numbers.
Identity Type	This field defaults to Named Principal and can't be modified. A named principal applies the same credential or authentication configuration for an entire org.
Authentication Parameters	Click Add to add your own Name and Value authentication parameters. Declaring them here alone doesn't do anything in a callout, but you can use authentication parameters as variables in request bodies and headers in Apex, and custom headers in named and external credentials. For example: <pre>{!\$Credential.SampleCustomExternalCredential.myAuthParam}</pre>

6. Save the principal.
You can't modify the Principal Name and Identity Type of an existing principal. To change these parameters, delete the principal and recreate it.
7. Map the principal to a permission set or profile. See [Enable External Credential Principals](#). You can map a principal to multiple permission sets, permission set groups, or profiles.

Congratulations—you've finished the main steps in creating a custom authentication external credential. See [Additional Tasks for External Credentials](#) for a few more jobs to complete.

Create and Edit a No Authentication External Credential

Follow these steps for creating an external credential if you're using no authentication.

Named credentials support making callouts to endpoints without any authentication protocol.

1. From Setup, enter *Named Credentials* in the Quick Find box, then select **Named Credentials**.
2. Click **External Credentials**.
3. To create a new external credential, click **New**. To edit an existing external credential, click its link in the list of external credentials and then click **Edit**.
4. Complete the fields.

Field	Description
Label	A user-friendly name for the external credential that's displayed in the Salesforce user interface, such as in list views.
Name	A unique identifier that's used to refer to this external credential from callout definitions and through the API. The name can contain only underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.
Authentication Protocol	Select No Authentication .

5. Save the external credential.

Create Principals for No Authentication Protocol

After you create an external credential that uses no authentication, create principals for it. To grant access, you map the principals to permission sets or profiles. A user making a callout must have permission to the principal.

1. On the Named Credentials page, click **External Credential**.
2. Select the external credential that you created.
3. Scroll to Principals.
4. To create a principal for the external credential, click **New** or select **Edit** from the Actions menu of an existing principal.
When editing an existing principal, not all the fields listed here are modifiable.
5. Enter the information for the principal.

Field	Description
Parameter Name	Enter a name for the principal, such as <i>Admin</i> or <i>Marketing Group</i> .
Sequence Number	Assign a sequence number. A sequence number specifies the order of principals to apply when a user participates in more than one principal. For example, a user could be part of multiple permission sets that are applicable for a credential provider. Priority is from lower to higher numbers.

EDITIONS

Available in: All Editions

USER PERMISSIONS

To view external credentials:

- View Setup and Configuration

To create, edit, or delete external credentials:

- Manage Named Credentials or Customize Applications

Field	Description
Identity Type	Set to Named Principal . Not editable. An external credential set up with named principal applies the same credential or authentication configuration for the entire org.

- Click **Save** to save the principal.
You can't modify the Principal Name and Identity Type of an existing principal. To change these parameters, delete the principal and recreate it.
- Map the principal to a permission set or profile. See [Enable External Credential Principals](#). You can map a principal to multiple permission sets, permission set groups, or profiles.

Congratulations—you've finished the main steps in creating an external credential with no authentication protocol. See [Additional Tasks for External Credentials](#) for a few more jobs to complete.

Create and Edit a JWT External Credential

Follow these steps for creating an external credential if you're using JWT authentication.

Named credentials support JWT authentication protocol for server-to-server integration.

- From Setup, enter *Named Credentials* in the Quick Find box, then select **Named Credentials**.
- Click **External Credentials**.
- To create a new external credential, click **New**. To edit an existing external credential, click its link in the list of external credentials and then click **Edit**.
- Complete the fields.

Field	Description
Label	A user-friendly name for the external credential that's displayed in the Salesforce user interface, such as in list views.
Name	A unique identifier that's used to refer to this external credential from callout definitions and through the API. The name can contain only underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.
Authentication Protocol	Select JWT . For complete list of JWT claims, see Set Up JWT Claims for Named Credentials .
Issuer (iss)	Specify who issued the JWT, which is a formula. For example, to return the Email ID, use the formula <code>{!\$User.Email}</code> .
Subject (sub)	Specify the subject of the token (the user), which is a formula.
Audience (aud)	Specify the recipient for whom the token is intended.

EDITIONS

Available in: All Editions

USER PERMISSIONS

To view external credentials:

- View Setup and Configuration

To create, edit, or delete external credentials:

- Manage Named Credentials or Customize Applications

Field	Description
JWT Expiration (Seconds)	Specify the time after which the token expires. Expressed as a NumericDate value, representing the number of seconds from 1970-01-01T00:00:00Z UTC until the specified UTC date/time, ignoring leap seconds.
Signing Certificate	Specify the certificate that's used to verify the JWT's authenticity to external systems.
Signing Algorithm	Specify the algorithm used to sign the token. Valid values are RS256 (default) and RS512.

5. Save the external credential.

Create Principals for JWT

After you create an external credential that uses JWT authentication, create principals for it. To grant access, you map the principals to permission sets or profiles. A user making a callout must have permission to the principal.

1. On the Named Credentials page, click **External Credential**.
2. Select the external credential that you created.
3. Scroll to Principals.
4. To create a principal for the external credential, click **New** or select **Edit** from the Actions menu of an existing principal.
When editing an existing principal, not all the fields listed here are modifiable.
5. Enter the information for the principal.

Field	Description
Parameter Name	Enter a name for the principal, such as <i>Admin</i> or <i>Marketing Group</i> .
Sequence Number	Assign a sequence number. A sequence number specifies the order of principals to apply when a user participates in more than one principal. For example, a user could be part of multiple permission sets that are applicable for a credential provider. Priority is from lower to higher numbers.
Identity Type	Choose either Named Principal or Per-User Principal . You can set up each external credential to use an org-wide named principal or per-user authentication. A named principal applies the same credential or authentication configuration for the entire org, while per-user authentication provides access control at the individual user level.

6. Click **Save** to save the principal.
You can't modify the Principal Name and Identity Type of an existing principal. To change these parameters, delete the principal and recreate it.
7. Map the principal to a permission set or profile. See [Enable External Credential Principals](#). You can map a principal to multiple permission sets, permission set groups, or profiles.

Congratulations—you've finished the main steps in creating a JWT external credential. See [Additional Tasks for External Credentials](#) for a few more jobs to complete.

Create and Edit a Basic Authentication External Credential

Follow these steps to create an external credential if you're using Basic authentication.

Named credentials support the Basic authentication protocol, which uses a static username and password to directly authenticate into the external system.

If the external system isn't compliant with standard authentication protocols, you can select a Custom authentication protocol for your external credential and use a custom header to authenticate. See [Using Basic Authentication with Named Credentials](#) on page 1187.

1. From Setup, in the Quick Find box, enter *Named Credentials*, and then select **Named Credentials**.
2. Click **External Credentials**.
3. To create a new external credential, click **New**. To edit an existing external credential, click its link in the list of external credentials, and then click **Edit**.
4. Complete the fields.

Field	Description
Label	A user-friendly name for the external credential that's displayed in the Salesforce user interface, such as in list views.
Name	A unique identifier that's used to refer to this external credential from callout definitions and through the API. The name can contain only underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.
Authentication Protocol	Select Basic Authentication .

5. Save the external credential.

Create Principals

After you create an external credential that uses the Basic authentication protocol, create principals for it. You link an external credential to permission sets or user profiles through principals, and at run time, the platform ensures that the user has the permission set before accessing the remote system.

1. On the Named Credentials page, click **External Credential**.
2. Select the external credential that you created.
3. Scroll to Principals.
4. To create a principal for the external credential, click **New** or select **Edit** from the Actions menu of an existing principal.
When editing an existing principal, not all the fields listed here are modifiable.
5. Enter the information for the principal.

EDITIONS

Available in: all editions

USER PERMISSIONS

To view external credentials:

- View Setup and Configuration

To create, edit, or delete external credentials:

- Manage Named Credentials or Customize Applications

Field	Description
Parameter Name	Enter a name for the principal, such as <i>Admin</i> or <i>Marketing Group</i> .
Sequence Number	Assign an optional sequence number. A sequence number specifies the order of principals to apply when a user participates in more than one principal. For example, a user can be part of multiple permission sets that are applicable for a credential provider. Priority is from lower to higher numbers.
Identity Type	Select Named Principal or Per-User Principal . A named principal applies the same credential or authentication configuration for the entire org, while per-user authentication provides access control at the individual user level. If you select Named Principal, also enter the username and password for accessing the external system. When you save the principal, the external credential is authorized automatically.

6. Save the principal.
You can't modify the Principal Name and Identity Type of an existing principal. To change these parameters, delete the principal and recreate it.
7. Map the principal to a permission set or profile. See [Enable External Credential Principals](#). You can map a principal to multiple permission sets, permission set groups, or profiles.
8. If the principal's Identity Type is Named Principal, the external credential is authorized automatically when you save the principal with the username and password. To authorize the external credential when the principal's Identity Type is set to Per User Principal, each user follows these steps.
 - a. From your personal settings, in the Quick Find box, enter *External Credentials*, and then select **External Credentials**.
 - b. In the tile of the external credential that you want to authenticate, click **Allow Access**.
 - c. Authenticate yourself to the external system. For example, enter a username and password.

The external credential is authenticated, and its tile shows Configured. To revoke authentication on an external credential, click **Revoke Access**.

Now that you created the external credential and mapped its principal to a permission set or profile, it's time to:

- Enable the user external credentials that Salesforce created automatically when you saved the principal. User external credentials store the encrypted authentication tokens used by named credentials, and you grant access so that users can access the tokens when they perform authenticated callouts. See [Enable User External Credentials](#).
- Create the name credential. See [Create and Edit a Named Credential](#).

Additional Tasks for External Credentials

After you created an external credential, there are a few more things to do to make the credential useful.

- Enable principal access for permission sets and profiles. See [Enable External Credential Principals](#).
- In addition to external credentials, the named credentials schema includes *user* external credentials. If you haven't done so already, make sure to grant permissions to access user external credentials. It's not necessary to enable user credentials every time you create an external credential. You enable access to user external credentials one time for each user or permission set. See [Enable User External Credentials](#).

EDITIONS

Available in: **All Editions**.

- Optionally, you can create custom headers for the external credential. Custom headers allow you to set your own parameters for authentication. See [Create and Edit Custom Headers](#).
- Create a named credential and link it to the external credential. See [Create and Edit a Named Credential](#).

Enable External Credential Principals

To make callouts that use a named credential, you must enable principal access to permission sets or profiles for the users who need access.

After you create principals and external credentials, take these steps to give permission sets and profiles access to the principals of the external credential.

 **Tip:** To apply credential permissions to the largest number of users, link a principal to a permission set and add the permission set to a permission set group.

1. From Setup, in the Quick Find box, enter either *Permission Sets* or *Profiles*, and then select either **Permission Sets** or **Profiles**.
2. Click the name of the permission set or profile that you want to modify.
3. Take one of these steps.
 - For a permission set, click **External Credential Principal Access** in the Apps section. Permission sets with external credential principal access enabled can be packaged.
 - For a profile, click **Enabled External Credential Principal Access**. Profiles associated with guest users are also supported.

4. Click **Edit**.

The Edit page displays two columns: one for available external credential principals, and one for external credential principals that are currently enabled.

External credential principals take the form

external credential name - external credential principal parameter name

For example, an external credential principal can have a name like 'JWT OAuth Credential - Marketing User'.

5. Select one or more external credential principals from the list of available principals. To move them into the Enabled column, click the **Add** arrow.
6. Save your changes.

User External Credentials

User external credential objects store encrypted tokens used by named credentials. You must enable user external credentials to use named credentials.

Named credentials reference external credentials, which specify authentication protocols and authorization information. In turn, external credentials use *user external credentials* to store encrypted authentication tokens. Any user performing an authenticated callout needs profile- or permission set-based access to user external credentials.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions**

Permission sets available in: **Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

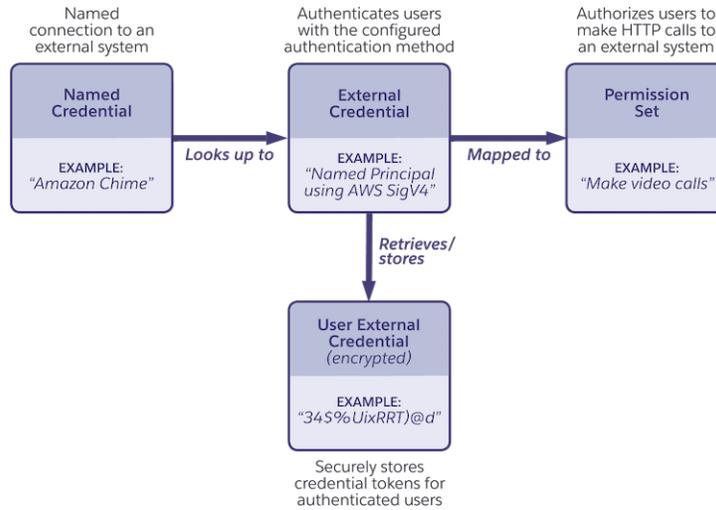
USER PERMISSIONS

To edit permission sets and user profiles:

- Manage Profiles and Permission Sets

EDITIONS

Available in: all editions



[Enable User External Credentials](#)

You must enable user external credentials so that users can make authenticated callouts using named credentials. There are two ways to enable user external credentials, via user profiles or permission sets. Which method you use depends on how you set up the associated external credential.

[Permission Concepts for User External Credentials](#)

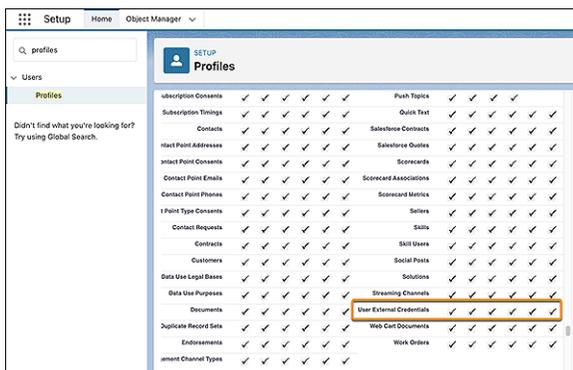
As a Salesforce admin, you must pay careful attention to security and permissions settings in your org. We recommend that you limit data access to the lowest level possible, while still allowing everyone to do their jobs. This strategy is known as the principle of least privilege. Whether you enable user external credentials via permission sets or profiles, follow this guidance to grant the appropriate access for each authentication protocol.

Enable User External Credentials

You must enable user external credentials so that users can make authenticated callouts using named credentials. There are two ways to enable user external credentials, via user profiles or permission sets. Which method you use depends on how you set up the associated external credential.

Enable User External Credentials Through User Profiles

Here's how to enable user external credentials through a user's profile.



EDITIONS

Available in: all editions

USER PERMISSIONS

To view external credentials:

- View Setup and Configuration

To create, edit, or delete external credentials:

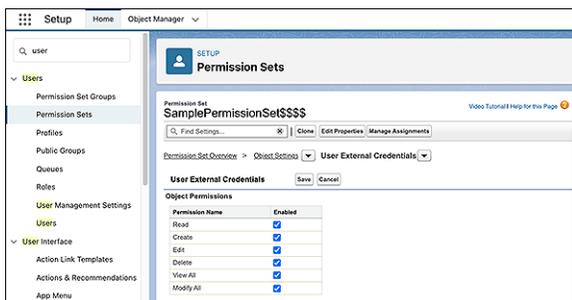
- Manage Named Credentials or Customize Applications

1. From Setup, in the Quick Find box, enter *Profiles*, and then select **Profiles**.
2. Click the profile for whom you want to enable user external credentials.
3. Scroll to Standard Object Permissions and select **User External Credentials**.
4. Check the boxes for the user external credential access that you want to give this user profile.
5. Save the settings.

You can grant guest user profiles read and create access to the user external credential and provide access to make callouts using named credentials.

Enable User External Credentials Through Permission Sets

Here's how to enable user external credentials by modifying a permission set for a user.



1. From Setup, in the Quick Find box, enter *permission sets*, and then select **Permission Sets**.
2. Click the permission set for which you want to enable user external credentials.
3. Under Apps, click **Object Settings**.
4. Click **User External Credentials**.
5. Click **Edit**, and assign the permissions that you want.
6. Save the settings.

You can't manipulate tokens directly. For example, you can't read them out or change them. You can, however, access user external credentials through the ConnectApi interface, just as you would with named credentials and external credentials.



Example: As an example, use `deleteCredential` to remove a user external credential and its associated tokens when an employee leaves a company. You provide the developer name of the external credential and the principal name and type associated with your credentials (the user external credential), and `deleteCredential` deletes all user external credentials for that principal.

```
String externalCredential = 'SampleExternalCredential';
String principalName = 'Principal';
ConnectApi.CredentialPrincipalType principalType =
ConnectApi.CredentialPrincipalType.NamedPrincipal;
```

```
ConnectApi.NamedCredentials.deleteCredential(externalCredential, principalName,
principalType);
```

SEE ALSO:

- [Apex Reference Guide: NamedCredentials Class](#)
- [Named Credentials and External Credentials](#)
- [Permission Concepts for User External Credentials](#)

Permission Concepts for User External Credentials

As a Salesforce admin, you must pay careful attention to security and permissions settings in your org. We recommend that you limit data access to the lowest level possible, while still allowing everyone to do their jobs. This strategy is known as the principle of least privilege. Whether you enable user external credentials via permission sets or profiles, follow this guidance to grant the appropriate access for each authentication protocol.

EDITIONS

Available in: all editions

User external credential objects store encrypted tokens used by named credentials to authenticate to external systems. In order to perform an authenticated callout, users need profile- or permission set-based access to user external credentials. These tables outline the necessary permissions for each authentication protocol. For more information about the authentication protocols, see [Authentication Protocols for Named Credentials](#) on page 1202.

OAuth 2.0

OAuth 2.0 Variant	Identity Type	Role	Access Level	Reason
<ul style="list-style-type: none"> • Browser Flow • JWT Bearer Flow • Client Credentials with JWT Assertion Flow • Client Credentials with Client Secret Flow 	Named Principal	Users making callouts	Modify All	<p>Users can make a callout using the access tokens entered by the admin.</p> <p>If a callout uses expired access tokens, the Modify All permission grants Salesforce access to retrieve refreshed tokens from the external system and update the external credential's principal with the new tokens on behalf of the user making the callout. Users can't access or update the named credential configuration in Setup.</p>
<ul style="list-style-type: none"> • Browser Flow • JWT Bearer Flow 	Per User Principal	Users making callouts	Read, Create, Edit, Delete	Each user can enter their credentials to authenticate to the external system, make callouts using the named credential, and revoke access, if needed.

AWS Signature Version 4

AWS Signature Version 4 Variant	Identity Type	Role	Access Level	Reason
Access Key and Secret	Named Principal	Salesforce admin	Read, Create, Edit, Delete	Only the admin can enter the access key and secret to authenticate to the external system or revoke access.
		Users making callouts	View All	Users can make a callout using the access key and secret entered by the admin. View All permission grants Salesforce access to the credentials for the external system on behalf of the user making a callout. Users can't access the named credential configuration in Setup.
<ul style="list-style-type: none"> • STS • IAM Roles Anywhere 	—	Users making callouts	Modify All	Users can make a callout using the access tokens entered by the admin. If a callout uses expired access tokens, the Modify All permission grants Salesforce access to retrieve refreshed tokens from the external system and update the external credential's principal with the new tokens on behalf of the user making the callout. Users can't access or update the named credential configuration in Setup.

Custom Authentication

The Custom authentication protocol supports only the Named Principal identity type. A named principal applies the same credential or authentication configuration for an entire org.

Role	Access Level	Reason
Salesforce admin	Read, Create, Edit, Delete	Only the admin can enter access tokens or API keys to authenticate to the external system or revoke access.
Users making callouts	View All	Users can make a callout using the access tokens entered by the admin. The View All permission grants Salesforce access to the credentials for the external system on behalf of the user making a callout. Users can't access the named credential configuration in Setup.

Basic Authentication

Identity Type	Role	Access Level	Reason
Named Principal	Salesforce admin	Read, Create, Edit, Delete	Only the admin can enter credentials to authenticate to the external system or revoke access.
	Users making callouts	View All	Users can make a callout using the credentials entered by the admin. The View All permission grants Salesforce access to the credentials for the external system on behalf of the user making a callout. Users can't access the named credential configuration in Setup.
Per User Principal	Users making callouts	Read, Create, Edit, Delete	Each user can enter their credentials to authenticate to the external system, make callouts using the named credential, and revoke access, if needed.

JWT

Identity Type	Role	Access Level	Reason
Named Principal	Users making callouts	Read	The Read permission grants users access to additional authentication parameters so that they can make callouts using the named credential.
Per User Principal	Users making callouts	Read	The Read permission grants users access to additional authentication parameters so that they can make callouts using the named credential.

No Authentication

The No Authentication protocol supports only the Named Principal identity type. A named principal applies the same credential or authentication configuration for an entire org.

Role	Access Level	Reason
Users making callouts	Read	The Read permission grants users access to additional authentication parameters so that they can make callouts using the named credential.

SEE ALSO:

[Named Credentials and External Credentials](#)

[Enable User External Credentials](#)

Custom Headers for Credentials

You can add custom headers to named credentials and external credentials. Custom headers are a way for a remote system to define parameters it needs as input to respond to a request. Using a custom header is similar to having a function in a piece of code and defining input parameters or arguments that allow the caller to provide input.

Because named credentials operate in the HTTP world, parameter provision is implemented as an HTTP request accompanied by headers that act as additional inputs required by the service you're calling. HTTP requests have a header and a body, and inputs can appear in both. It's also common for inputs to appear in a URL as a query string. All three approaches have pros and cons. We only discuss headers here.

Custom headers are most often used for security or authentication purposes. The HTTP standard includes a commonly used, dedicated Authorization header. However, many use cases require something else. Two common use cases are per-user callouts and API keys.

EDITIONS

Available in: **All Editions**

Per-User Callouts

Many systems respond to HTTP requests differently based on which user, or role, makes the request. For example, sometimes an integration to a company returns a personal phone number, but only if the person whose phone number it's makes that callout request. However, a calling user in the company's HR department can see any user's salary, though the HR role must be specified.

Here's an example of a per-user callout that uses a custom header to identify the user by their email address.

```
GET https://example.com/getInfo?personId=my_username%40example.com/HTTP/1.1
X-Calling-User:my_username@example.com
```

As another example, Microsoft offers an enterprise-wide search service and returns different results based on the caller's identity. (Users don't get results they're not allowed to see.) Salesforce named credentials support this service because administrators can define headers like `X-Calling-User` and substitute the value of the user making the callout, for example `{!$User.email}`. The header is defined on an external credential in a manner similar to the next example.



Tip: If you're using a formula in a custom header in an external credential, and you chose Named Principal as your Identity Type, don't use `$User` in the formula.

API Keys

"API key" refers to a programmatic password used in an HTTP request to identify a calling application attempting to access a given API. API keys have no strict standard, so anyone who builds an API can define their own headers, rules, and so on.

```
GET https://example.com/api/11a5aea0?count=20 HTTP/1.1
X-API-Key: abc123
```

`X-API-Key` is arbitrary, and some vendors use headers like `Client-ID`. This example, for retrieving a random photograph, uses a mixture of `Client-ID` and the standard Authorization header.

```
GET https://example.com/photos/random_HTTP/1.1
Authorization: Client-ID abc123
```

Here's what an external credential that uses a custom header with an API key can look like.

The screenshot shows the configuration page for a Named Credential. At the top, it says 'SETUP > NAMED CREDENTIALS' and 'Stock Photo Client App'. There are 'Edit' and 'Delete' buttons. Below this, the configuration details are shown:

- Label:** Stock Photo Client App
- Name:** testname__StockPhotoClientApp
- Authentication Protocol:** Custom

Below the configuration details is a section for 'Related Named Credentials' with a table:

Label	Name	URL
Random Stock Photo	testname__RandomStockPhoto	https://example.com/photos/random_HTTP/1.1

Next is the 'Principals' section with a 'New' button and a table:

Sequ...	Parameter Name	Authe...	Actions
1	Load Stock Photos	0	

Finally, there is a 'Custom Headers' section with a 'New' button and a table:

S	Name	Value	Actions
1	Authorization	{!Client-ID ' & \$Credential.MyCustAuthExternCred.MyClientId}	

- The credential uses a custom authorization protocol.
- It uses a Load Stock Photos principal.
- It's linked to a named credential, Random Stock Photo, that can have its own custom header.
- `AccessKey` is defined in the principal.

For more on using API keys, see [Use API Keys with Named Credentials](#).

Custom Headers in Named Credentials and External Credentials

You can use custom headers in named and external credentials. If you create custom headers for both, a single callout combines them.

- For popular use cases like the examples here, it's best to associate headers with the external credential, rather than the named credential, because external credentials are meant to encapsulate authentication details. For example, define custom authorization headers in an external credential to use consistent authentication across all named credential endpoints using the same external credential.
- Define custom headers at the level of a named credential if the headers are contextual to a single endpoint. An example of a header that works better on a named credential is a billing identifier. In all likelihood, this type of identifier has nothing to do with authentication or security, and it can be different for each endpoint.

```
GET https://example.com/method?abc=def HTTP/1.1
X-Billing-Code: costCenter123
```

- Headers from named credentials are placed before headers from external credentials.
- Headers from named credentials overwrite headers from external credentials if the names duplicate.
- Headers can have duplicate header names if they're from the same source.

[Create and Edit Custom Headers](#)

Use custom headers to make unique secure connections to external data sources. You can add custom headers to both named credentials and external credentials.

[Use API Keys with Named Credentials](#)

Web services often define their own authentication protocols using custom headers. For those cases, you can create a custom header for a named or external credential and use API keys as a password.

[Using Basic Authentication with Named Credentials](#)

Create an external credential with a custom header that uses HTTP Basic authentication.

[Named Credential Formula Functions](#)

Formula functions can be used in the value field of a custom header of a named credential or external credential.

Create and Edit Custom Headers

Use custom headers to make unique secure connections to external data sources. You can add custom headers to both named credentials and external credentials.

For more on custom headers, see [Custom Headers for Credentials](#) and [Custom Headers and Bodies of Apex Callouts That Use Named Credentials](#).

Salesforce generates a standard authorization header for each callout to a named-credential-defined endpoint. If you're creating a custom header, disable **Generate Authorization Header** in the associated named credential.

Note the following when creating custom headers.

- Headers are sorted by source and sequence number. Headers from named credentials are placed before headers from external credentials.
 - Headers from named credentials overwrite headers from external credentials if the names duplicate.
 - Headers are allowed to have duplicate header names if they're from the same source.
1. From Setup, enter *Named Credentials* in the Quick Find box, then select **Named Credentials**.
 2. Click either **Named Credentials** or **External Credentials**.
 3. If you're creating a custom header, click **New**. If you're editing an existing custom header, select **Edit** from the Actions menu dropdown for that header.
 4. Fill in the fields for the custom header.

EDITIONS

Available in: **All Editions**

USER PERMISSIONS

To view named credentials:

- View Setup and Configuration

To create, edit, or delete named credentials:

- Manage Named Credentials or Customize Applications

Field	Description
Name	The name of the custom header for this credential.
Value	The value of the header, evaluated as a formula. For more on setting custom header values, see Use API Keys with Named Credentials , Using Basic Authentication with Named Credentials , and Named Credential Formula Functions . If you're using a formula in a custom header and you've chosen Named Principal as your Identity Type, don't use <code>user</code> in the formula.
Sequence Number	A number that determines the order in which headers are sent out in the callout. Headers with lower numbers are sent out first.

5. Click **Save** to save the custom header.

Use API Keys with Named Credentials

Web services often define their own authentication protocols using custom headers. For those cases, you can create a custom header for a named or external credential and use API keys as a password.

The named credentials schema includes support for authentication protocols like OAuth 2.0 and AWS Signature v4. Some web service providers have their own authentication protocols that use unique headers for authentication. In these cases, choose a `Custom` authentication protocol for your external credential, and use a custom header to authenticate to such systems.

One common approach used by web service providers for custom authentication is *API keys*. Besides authentication, API keys can also be used for various HTTP-related services, such as caching or cookies. For named credentials, you can create a custom header that uses API keys as an authentication protocol, with the key's secret value functioning as a password.

Each web service can name its headers arbitrarily. Common names include `ACCESS_TOKEN`, `bearer`, `Client-ID`, `developer-token`, and `X-API-Key`.

For the HTTP 1.x standard, a call using a (hard-wired) API key can look something like this.

```
GET https://example.com HTTP/1.1
Client-ID: abc123
```

Here the API key `Client-ID` is also the name of the header, and `abc123` is the value of the API key used for authentication. The name and the value are set by the authenticating system. Typically, you retrieve these parameters through the external system's UI.

The HTTP standard includes an `Authorization` header for authentication. By default, Salesforce named credentials use this standard authorization header. However, you can override the default and create a custom `Authorization` header. This example shows the `Authorization` header used with an API key.

```
GET https://example.com HTTP/1.1
Authorization: Client-ID abc123
```

The general steps to using API keys with named credentials are:

1. Create an external credential, setting the Authentication Protocol to `Custom`. An external credential stores authentication and authorization information and is used by named credentials.
2. Store the API key as an authorization parameter in a principal.
3. Create a custom header for the external credential. The header references the API key.
4. Create a named credential that references the external credential.

Store an API Key as an Authentication Parameter in a Principal

We strongly recommend storing API key authentication parameters as part of an external credential principal.

The API key is a secret value. Authentication parameters are expected to contain secrets and are stored in an encrypted manner consistent with other sensitive information. Additionally, access to the secrets is granted explicitly using a principal.

A principal links an external credential to permission sets and profiles. By adding authentication parameters to a principal, you enable different groups of Salesforce users to use different authentication tokens to call the same external service.

1. Create an external credential and set the Authentication Protocol field to **Custom**. For instructions on creating and configuring external credentials, see [Create and Edit a Custom Authentication External Credential](#). In this example, the external credential is named `MyCustAuthExternCred`.

EDITIONS

Available in: **All Editions**

2. On the external credential's page, scroll to Principals.
3. To create a principal, click **New**, and set these fields.

Parameter Name

A name for the principal, such as *Admin* or *Marketing Team*.

Sequence Number

This number determines which mapping is used for the callout, sorted from lowest to highest. Set the sequence number in case a user has multiple permission sets used in multiple principals.

Identity Type

Custom authentication uses the Named Principal identity type. Named Principal indicates that Salesforce users share the same API key, and they don't have unique access to the external service. You can't change the identity type for Custom authentication.



Note: At this time, only the OAuth protocol supports unique per-user access to a remote system. In that case, each user logs in separately before the integration works in their user context.

Name

The name for the authentication parameter. In this example, the name is `MyClientId`.

Value

The API key value. In many cases, you get the API key from the web service's UI.

4. Map the principal to a permission set or profile. See [Enable External Credential Principals](#). You can map a principal to multiple permission sets, permission set groups, or profiles.

Use API Keys in a Custom Header

After you've added API keys to a principal, you can use those keys in a custom header.

1. On the external credential that you created, scroll to Custom Headers and click **New**.
2. Fill in the fields for the custom header.

The screenshot shows a 'Create Custom Header' dialog box. It contains three input fields:

- Name:** Authorization
- Value:** {!Client-ID ' & \$MyCustAuthExternCred.MyClientId}
- Sequence Number:** 1

 At the bottom right, there are 'Cancel' and 'Save' buttons. The dialog is titled 'Create Custom Header' and has a close button (X) in the top right corner. The background shows a list of 'Custom Headers'.

Name

The name of the standard HTTP request header as required by the external service. In this case we're performing authentication, so we use the HTTP standard name 'Authorization'.

Value

The API key name and value. It can be a literal or a programmatic expression.

The value can be expressed programmatically with merge fields and formulas. For instance, the value can take the form:

```
{!'Client-ID ' & $Credential.Container.ParameterName}
```

where the literal string `Client-ID` is concatenated with the API key. In our example, this expression resolves as:

```
{!'Client-ID ' & $Credential.MyCustAuthExternCred.MyClientId}
```

Formulas can be used in header values via the `{!FormulaGoesHere}` syntax. Anything inside `{!}` is evaluated as a Salesforce formula. Formulas provide significant power and flexibility to craft header values without coding.

Merge fields provide access to encrypted values via the `$Credential.Container.ParameterName` syntax. In this example `Container` is the external credential `MyCustAuthExternCred`. `ParameterName` is the principal authentication parameter `MyClientId`, which was mapped to the API key value.

Sequence Number

This number determines which header "wins" and gets used for the callout, sorted from lowest to highest. If you're not worried about collisions with other headers, leave this field as the default.

The external credential now shows the custom header with a reference to the authorization parameter that contains the API key.

SETUP > NAMED CREDENTIALS

My Custom Auth External Credential Edit Delete

Label: My Custom Auth External Credential Name: testname__MyCustAuthExternCred

Authentication Protocol: Custom

Related Named Credentials

Label	Name	URL
My Custom Auth Named Credential	testname__MyCustAuthNamedCred	https://www.example.com

Principals New

Seque...	Parameter Name	Authen...	Actions
1	Marketing Team	1	

Custom Headers New

S	Name	Value	Actions
1	Authorization	{!Client-ID' & \$Credential.MyCustAuthExternCred.MyClientId}	

If `Client-ID` is `abc123`, the resulting callout looks like this. The named credential appends 'Authorization:' as the header name.

```
GET https://example.com HTTP/1.1
Authorization: Client-ID abc123
```



Tip: Make sure you've enabled user external credentials for your users who are using named credentials. See [Enable User External Credentials](#).

Use API Keys with a Named Credential

After you've created an external credential that uses API keys, it can be referenced by a named credential.

A callout using this named credential returns successfully because it has the correct `Authorization` header. If the tokens expire or the URL changes, no changes to Apex code are needed. In addition to Apex, the credential can be used in no-code tools like External Services that provide integration with Flow.

1. Disable **Generate Authorization Header** in the named credential. Disabling this option ensures that the named credential uses the custom `Authorization` header that you created.
2. In that named credential, make sure that **Allow Formulas in HTTP Header** is enabled.

A callout using this Named Credential returns successfully because it has the correct `Authorization` header. If the tokens expire or the URL changes, no changes to Apex code are needed. In addition to Apex, the credential can be used in no-code tools like External Services that provide integration with Flow.

For more on creating and configuring named credentials, see [Create and Edit a Named Credential](#).

SEE ALSO:

[Custom Headers for Credentials](#)

[Calculate Field Values With Formulas](#)

[Apex Developer Guide: Merge Fields for Apex Callouts That Use Named Credentials](#)

Using Basic Authentication with Named Credentials

Create an external credential with a custom header that uses HTTP Basic authentication.

The named credentials schema includes support for authentication protocols like OAuth 2.0 and AWS Signature v4. Some web service providers, however, have their own authentication protocols that use unique headers for authentication. One such protocol is the HTTP Basic authentication scheme, a simple username-password protocol. To connect to an external service using Basic authentication, choose a `Custom` authentication protocol for your external credential, and use a custom header to authenticate.

The HTTP Basic authentication scheme uses the `Authorization` HTTP header, along with a username and password combined using base64 encoding. The username and password are concatenated with a colon (:), then encoded.

EDITIONS

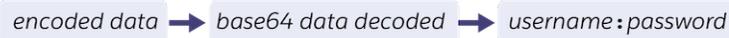
Available in: **All Editions**



For example:

```
myUsername:myPassword → base64 encoding → bX1Vc2VybmFtZTpteVBhc3N3b3JkCg==
```

The username and password can be similarly decoded.



Example:

```
bX1Vc2VybmFtZTpteVBhc3N3b3JkCg== → base64 data decoded → myUsername:myPassword
```

⚠ Important: The Basic system *encodes* the username and password, but it doesn't *encrypt* them. Because the username and password can be decoded by anyone who encounters them, the Basic authentication scheme is only secure when used with SSL encryption (HTTPS/TLS).

The encoded Basic data goes in the `Authorization` header as follows.

```
GET https://example.com HTTP/1.1
Authorization: Basic bX1Vc2VybmFtZTpteVBhc3N3b3JkCg==
```

Create a Custom Header for Basic Authentication

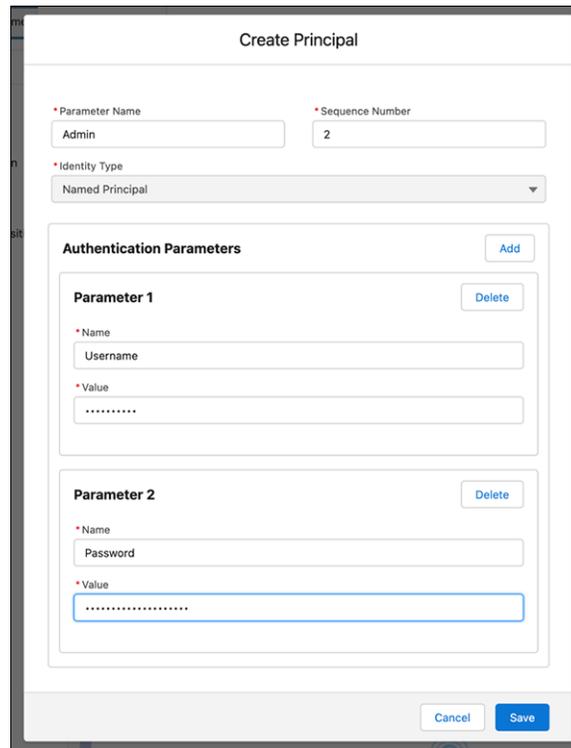
Both named and external credentials can have custom credentials. To create a custom header for Basic authentication, use an external credential.

Here's a general outline of how to use named credentials with a custom `Authorization` header that uses Basic authentication. For more detailed information on how to create external credentials with custom headers, see [Create and Edit an External Credential](#).

1. Create an external credential. Give it a name like 'BasicAuth'.
2. Set the credential's authentication protocol to **Custom**. Save the external credential.
3. Scroll to Principals and click **New**.
The new principal automatically has an identity type of Named Principal, which can't be changed.
4. Enter a **Parameter Name**, such as *Admin* or *Marketing Group*.
5. Optionally, enter a sequence number.

- Under Authentication Parameters, click **Add** to add a parameter, for example `Username`. Set the value to the username you use for the web service provider. Click **Add** again to add another parameter, for instance `Password`, and set it as the password you use for the web service provider.

 **Note:** Some systems don't use passwords for Basic authentication. For example, when authenticating to GitHub, you use a personal access token instead of your user password.



- Save the principal.
- Now create a custom header with a formula for an encoded Basic username-password combination. (See [Create and Edit Custom Headers](#) for more on creating custom headers.) On the external credential, scroll to Custom Headers and click **New**.
- Enter `Authorization` as the name of the custom header.
- For **Value**, enter:

```
{!'Basic ' & BASE64ENCODE(BLOB($Credential.externalCredentialName.Username & ':' & $Credential.externalCredentialName.Password)) }
```

where `externalCredentialName` is the name of the external credential you created ('BasicAuth' in this example).

Base64 encoding is often used to convert binary data to a text string for easier transfer between systems. Binary data stored in some databases is sometimes referred to as a Binary Large Object (BLOB). Two formulas, `BLOB` and `BASE64ENCODE`, used together, take the secret values, treat them as binary data, and then encode that binary data with base64. For more information on formula functions like `BASE64ENCODE`, see [Named Credential Formula Functions](#).

- Set the sequence number as desired, or leave the default.
- Save the custom header.

Use Basic Authentication with a Named Credential

After you've created an external credential that uses custom headers with Basic authentication, link it to a named credential.

These steps describe the general process of linking Basic authentication to a named credential. For full instructions on creating and editing named credentials, see [Create and Edit a Named Credential](#).

1. From Setup, in the Quick Find box, enter *Named Credentials*, and then select **Named Credentials**.
2. Create a new named credential or select an existing one.
3. Disable **Generate Authorization Header** in the named credential. Disabling this option ensures that the named credential uses the custom `Authorization` header that you created.
4. In the named credential, be sure that **Allow Formulas in HTTP Header** is enabled.
5. Enter the name of the external credential that uses Basic authentication.
6. Save the named credential.

A callout using this named credential returns successfully because it has the correct `Authorization` header. If the tokens expire or the URL changes, no changes to Apex code are needed. In addition to Apex, the credential can be used in no-code tools like External Services that provide integration with Flow.

SEE ALSO:

- [Custom Headers for Credentials](#)
- [Calculate Field Values With Formulas](#)
- [External Services](#)
- [Use Flow to Invoke External Service Actions](#)

Named Credential Formula Functions

Formula functions can be used in the value field of a custom header of a named credential or external credential.

 **Note:** Not all Salesforce formula functions are supported for named and external credential custom headers. We recommend using these formula functions for authentication use cases.

A binary large object (BLOB) is a collection of binary data stored as a single entity. For named credentials, BLOBs can store binary executable code used in custom header formulas.

EDITIONS

Available in: all editions

Table 14: Formula Functions for Named Credentials

Function	Description
<code>BASE64DECODE(expr)</code>	<p>Input String</p> <p>Output BlobValue</p> <p>Description Decode the Base64-encoded String expression to a binary.</p>
<code>BASE64ENCODE(expr)</code>	<p>Input BlobValue</p>

Function	Description
	<p>Output String</p> <p>Description Encode the binary BLOB expression as a Base64-encoded String.</p>
BLOB(<i>expr</i>)	<p>Input String</p> <p>Output BlobValue</p> <p>Description Convert the value to a UTF-8 binary BLOB.</p>
HASH(<i>algorithm, expr</i>)	<p>Input String, BlobValue</p> <p>Output BlobValue</p> <p>Description Given a binary value to hash, use <i>algorithm</i> to get the binary hash. The only supported hashing algorithm is SHA-256.</p>
HEX(<i>expr</i>)	<p>Input BlobValue</p> <p>Output String</p> <p>Description Represents the given BLOB expression as a base-16 lower-case encoded String. This hex encoding contains the binary data expected by encryption functions.</p>
HMAC(<i>algorithm, valueToSign, secretSigningKey</i>)	<p>Input String, BlobValue, BlobValue</p> <p>Output BlobValue</p> <p>Description Use <i>algorithm</i> to sign the given binary <i>valueToSign</i> with a binary secret signing key. The resulting message authentication code is a binary value. The only supported algorithm is SHA-256.</p>
SIGN(<i>algorithmName, input, privateKey</i>)	<p>Input String, BlobValue, BlobValue</p>

Function	Description
	<p>Output BlobValue</p> <p>Description Compute a unique digital signature for the input string using the specified algorithm and private key.</p> <p>Supported algorithms are RSA, RSA-SHA1, RSA-SHA256, RSA-SHA384, RSA-SHA512, ECDSA-SHA256, ECDSA-SHA384, and ECDSA-SHA512.</p>
SIGN_WITH_CERTIFICATE(<i>algorithmName</i> , <i>input</i> , <i>certDevName</i>)	<p>Input String, BlobValue, String</p> <p>Output BlobValue</p> <p>Description Compute a unique digital signature for the input string using the specified algorithm and the unique name of a certificate in the Salesforce org.</p> <p>Supported algorithms are RSA, RSA-SHA1, RSA-SHA256, RSA-SHA384, RSA-SHA512, ECDSA-SHA256, ECDSA-SHA384, and ECDSA-SHA512.</p>

Examples

- This example shows encoding a username and password stored in an external credential. The `BLOB` function first converts a string of form `username:password` into a binary. `BASE64ENCODE` then converts the binary into an encoded string. `myExternalCredential` is the name of an external credential.

```
BASE64ENCODE (BLOB ($Credential.myExternalCredential.Username & ':' &
$Credential.myExternalCredential.Password))
```

- This example sets a header named `X-Username` with a base-16, SHA-256-hashed username as the value. `req` is an `HttpRequest`. `Username` is an authentication parameter attached to a principal.

```
req.setHeader('X-Username', '{!HEX (HASH (\ 'SHA-256\' ,
BLOB ($Credential.myExternalCredential.Username)) )}');
```

- This example sets the `X-Body` header as the base-16, hashed *evaluated* body, meaning that all formulas within the request body are evaluated. `BLOB` isn't required here because `$$Credential.myExternalCredential.Body` is returned as a `BLOB` type rather than as a `String`.

```
req.setHeader('X-Body', '{!HEX(HASH(\ 'SHA-256\ ',
$Credential.myExternalCredential.Body))}');
```

SEE ALSO:

[Using Basic Authentication with Named Credentials](#)

[Formula Operators and Functions by Context](#)

[Calculate Field Values With Formulas](#)

[Apex Developer Guide: Merge Fields for Apex Callouts That Use Named Credentials](#)

Create and Edit a Named Credential

A named credential specifies the URL of a callout endpoint and its required authentication parameters in one definition. A named credential can be specified as an endpoint to simplify the setup of authenticated callouts. Named credentials connect to external credentials.

Before creating a named credential, create an external credential to link it to. See [Create and Edit an External Credential](#).

- From Setup, enter *Named Credentials* in the Quick Find box, then select **Named Credentials**.
- Click **Named Credentials**.
- To create a new named credential, click **New**. To edit an existing named credential, click its link in the list of named credentials and then click **Edit**.

 **Note:** If you want to create a legacy named credential, select **New Legacy** from the dropdown menu instead and follow the instructions in [Define a Legacy Named Credential](#). Legacy named credentials are deprecated and will be unsupported in a future release.

- Complete the fields.

Field	Description
Label	A user-friendly name for the named credential that's displayed in the Salesforce user interface, such as in list views.
Name	A unique identifier that's used to refer to this named credential from callout definitions and through the API. The name can contain only underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.
URL	The URL or root URL of the callout endpoint. Must begin with <code>https://</code> . Can include a path but not a query string. For example: <code>https://my_endpoint.example.com/secure/payroll</code>

EDITIONS

Available in: **All Editions**

USER PERMISSIONS

To view named credentials:

- View Setup and Configuration

To create, edit, or delete named credentials:

- Manage Named Credentials or Customize Applications

Field	Description
	<p>You can, however, append a query string and a specific path in the callout definition's reference to the named credential.</p> <p>For example, an Apex callout could reference the named credential "My_Payroll_System" as follows.</p> <pre>HttpRequest req = new HttpRequest(); req.setEndpoint('callout:My_Payroll_System/paystubs?format=json');</pre>
Enabled for Callouts	By default, the ability to make callouts with the named credential is turned on. The exception is when the named credential is created from applications written in Apex, in which case it's turned off. Be aware of security considerations when enabling callouts for named credentials that originate from Apex.
Authentication	
External Credential	The name of an external credential. See Create and Edit an External Credential .
Client Certificate	Optional. If you specify a certificate, your Salesforce org supplies it when establishing each two-way SSL connection with the external system. The certificate is used for digital signatures, which verify that requests are coming from your Salesforce org.
Callout Options	
Generate Authorization Header	<p>By default, Salesforce generates an authorization header and applies it to each callout that references the named credential.</p> <p>Deselect this option only if one of the following statements applies.</p> <ul style="list-style-type: none"> The remote endpoint doesn't support authorization headers. You're generating an authorization header by creating a custom header and naming it 'Authorization'. For example, create a custom authorization header if you're using HTTP Basic authorization. Likewise, in Apex callouts, you can have the code construct a custom authorization header for each callout. <p>This option is required if you reference the named credential from an external data source. See Custom Headers and Bodies of Apex Callouts That Use Named Credentials.</p>
Allow Formulas in HTTP Header	<p>Use credential fields as formula fields in named credential custom headers, external credential custom headers, and Apex HTTP headers. For example:</p> <pre>Client-ID: {!\$Credential.MyExtCred.MyClientId}</pre> <p>Defaults to false. See Custom Headers and Bodies of Apex Callouts That Use Named Credentials.</p>
Allow Formulas in HTTP Body	Allow Apex to construct the callout's HTTP body with credential fields available as formula fields. Defaults to false. See Custom Headers and Bodies of Apex Callouts That Use Named Credentials .
Outbound Network Connection	<p>Use a private connection that bypasses the public internet. Enter the name of an existing outbound network connection. See Secure Cross-Cloud Integrations with Private Connect.</p> <p>If you choose this option, your new named credential has <code>PrivateEndpoint</code> as its type. Otherwise the named credential has a <code>SecuredEndpoint</code> type.</p>

Field	Description
Allowed Namespaces for Callouts	<p>Optional list of namespaces that identifies the managed packages that are allowed to make callouts using this named credential.</p> <ul style="list-style-type: none"> For managed packages, the subscriber must add the package’s namespace to a named credential’s list of allowed namespaces to enable callouts. This action isn’t necessary if the named credential is installed as part of the same package. If you have multiple orgs, you can create a named credential with the same name but with a different endpoint URL in each org. You can then package and deploy—on all the orgs—one callout definition that references the shared name of those named credentials. For example, the named credential in each org can have a different endpoint URL to accommodate differences in development and production environments. If an Apex callout specifies the shared name of those named credentials, the Apex class that defines the callout can be packaged and deployed on all those orgs without programmatically checking the environment. <p>Named credentials aren’t automatically added to packages. If you package an external data source or Apex code that specifies a named credential as a callout endpoint, add the named credential to the package. Alternatively, make sure that the subscriber org has a valid named credential with the same name.</p>

5. Click **Save**. You’re taken to the Named Credentials screen.

6. Optionally, create a custom header for this named credential or edit an existing custom header. See [Create and Edit Custom Headers](#).

If you haven’t done so, enable user external credentials for all users who are using named credentials. See [Enable User External Credentials](#).

To reference a named credential from a callout definition, use the named credential URL. A named credential URL contains the scheme `callout:`, the name of the named credential, and an optional path. For example:

```
callout:My_Named_Credential/some_path.
```

You can append a query string to a named credential URL. Use a question mark (?) as the separator between the named credential URL and the query string. For example: `callout:My_Named_Credential/some_path?format=json`.

SEE ALSO:

[Create and Edit an External Credential](#)

[Custom Headers for Credentials](#)

[Metadata API: NamedCredential](#)

[Tooling API: NamedCredential](#)

Legacy Named Credentials

A legacy named credential specifies the URL of a callout endpoint and its required authentication parameters in one definition. Legacy named credentials are deprecated and are unsupported in future releases.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **All** Editions

 **Important:** In Winter '23, Salesforce introduced an improved named credential that is extensible and customizable. We strongly recommend that you use this preferred credential instead of legacy named credentials. For information on extensible, customizable named credentials, see [Named Credentials and External Credentials](#). Legacy named credentials are deprecated and will be discontinued in a future release.

To simplify the setup of authenticated callouts, specify a legacy named credential as the callout endpoint. If you instead specify a URL as the callout endpoint, you must register that URL in your org's remote site settings and handle the authentication yourself. For example, for an Apex callout, your code handles authentication, which can be less secure and especially complicated for OAuth implementations.

Salesforce manages all authentication for callouts that specify a legacy named credential as the callout endpoint so that you don't have to. You can also skip remote site settings, which are otherwise required for callouts to external sites, for the site defined in the legacy named credential.

 **Note:** All credentials stored within the `NamedCredential`, `ExternalDataSource`, and `ExternalDataUserAuth` entities are encrypted under a framework that is consistent with other encryption frameworks on the platform. Salesforce encrypts your credentials by auto-creating org-specific keys.

Legacy named credentials are supported in these types of callout definitions:

- Apex callouts
- External data sources of these types:
 - Salesforce Connect: OData 2.0
 - Salesforce Connect: OData 4.0
 - Salesforce Connect: Custom (developed with the Apex Connector Framework)
 - Salesforce Connect: Amazon DynamoDB
- External Services

Legacy named credentials include an `OutboundNetworkConnection` field that you can use to route callouts through a private connection. By separating the endpoint URL and authentication from the callout definition, legacy named credentials make callouts easier to maintain. For example, if an endpoint URL changes, you update only the legacy named credential. All callouts that reference the legacy named credential simply continue to work.

If you have multiple orgs, you can create a legacy named credential with the same name but with a different endpoint URL in each org. You can then package and deploy—on all the orgs—one callout definition that references the shared name of those legacy named credentials. For example, the legacy named credential in each org can have a different endpoint URL to accommodate differences in development and production environments. If an Apex callout specifies the shared name of those legacy named credentials, the Apex class that defines the callout can be packaged and deployed on all those orgs without programmatically checking the environment.

Legacy named credential authentication protocols include basic password authentication, OAuth 2.0, JWT, JWT Token Exchange, and AWS Signature Version 4. You can set up each legacy named credential to use an org-wide named principal or per-user authentication. A named principal applies the same credential or authentication configuration for the entire org, while per-user authentication provides access control at the individual user level.

To reference a legacy named credential from a callout definition, use the legacy named credential URL. A legacy named credential URL contains the scheme `callout:`, the name of the legacy named credential, and an optional path. For example:

```
callout:My_Named_Credential/some_path.
```

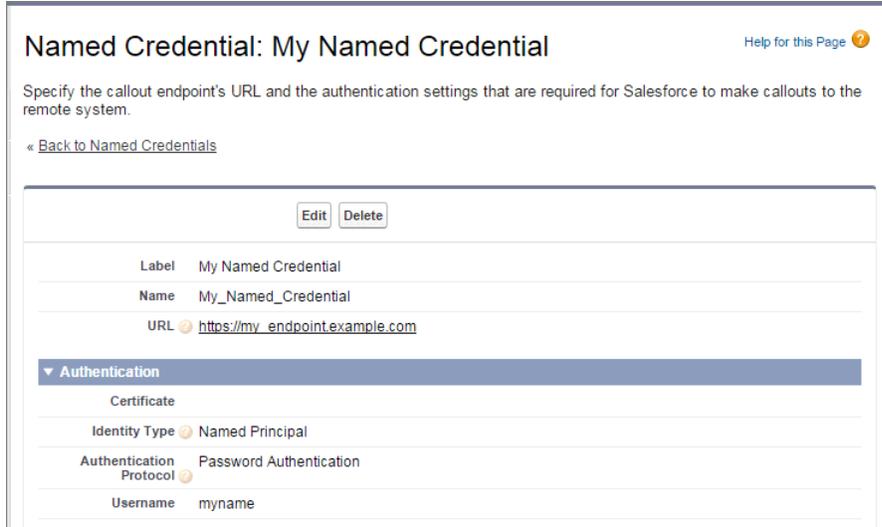
You can append a query string to a legacy named credential URL. Use a question mark (?) as the separator between the legacy named credential URL and the query string. For example: `callout:My_Named_Credential/some_path?format=json`.

 **Note:** If transmitting sensitive information such as healthcare data or credit card data, authenticated legacy named credentials are required. We recommend that customers provide their own certificates for extra security of sensitive data transmissions.

 **Example:** In the following Apex code, a legacy named credential and an appended path specify the callout's endpoint.

```
HttpRequest req = new HttpRequest();
req.setEndpoint('callout:My_Named_Credential/some_path');
req.setMethod('GET');
Http http = new Http();
HTTPResponse res = http.send(req);
System.debug(res.getBody());
```

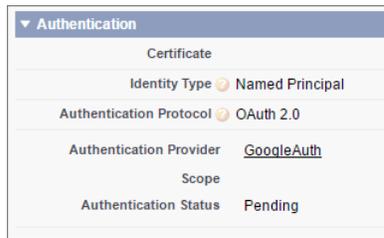
The referenced legacy named credential specifies the endpoint URL and the authentication settings.



The screenshot shows the configuration page for a named credential. The title is "Named Credential: My Named Credential". Below the title is a description: "Specify the callout endpoint's URL and the authentication settings that are required for Salesforce to make callouts to the remote system." There is a "Back to Named Credentials" link. The configuration fields are as follows:

Label	My Named Credential
Name	My_Named_Credential
URL	https://my_endpointexample.com
Authentication	
Certificate	
Identity Type	Named Principal
Authentication Protocol	Password Authentication
Username	myname

If you use OAuth instead of password authentication, the Apex code remains the same. The authentication settings differ in the legacy named credential, which references an authentication provider that's defined in the org.



The screenshot shows the authentication settings for a named credential. The settings are as follows:

Authentication	
Certificate	
Identity Type	Named Principal
Authentication Protocol	OAuth 2.0
Authentication Provider	GoogleAuth
Scope	
Authentication Status	Pending

In contrast, let's see what the Apex code looks like without a legacy named credential. Notice that the code becomes more complex to handle authentication, even if we stick with basic password authentication. Coding OAuth is even more complex and is an ideal use case for legacy named credentials.

```
HttpRequest req = new HttpRequest();
req.setEndpoint('https://my_endpoint.example.com/some_path');
req.setMethod('GET');

// Because we didn't set the endpoint as a legacy named credential,
// our code has to specify:
// - The required username and password to access the endpoint
// - The header and header information
```

```
String username = 'myname';
String password = 'mypwd';

Blob headerValue = Blob.valueOf(username + ':' + password);
String authorizationHeader = 'BASIC ' +
EncodingUtil.base64Encode(headerValue);
req.setHeader('Authorization', authorizationHeader);

// Create a new http object to send the request object
// A response object is generated as a result of the request

Http http = new Http();
HTTPResponse res = http.send(req);
System.debug(res.getBody());
```

[Define a Legacy Named Credential](#)

Create a legacy named credential to specify the URL of a callout endpoint and its required authentication parameters in one definition. You can then specify the legacy named credential as a callout endpoint to let Salesforce handle all authentication. You can also skip remote site settings, which are otherwise required for callouts to external sites, for the site defined in the legacy named credential.

[Grant Access to Authentication Settings for Legacy Named Credentials](#)

For legacy named credentials that use per-user authentication, grant access to users through permission sets and profiles. Doing so lets users set up and manage their own authentication settings for accessing the external system.

SEE ALSO:

[Authentication Protocols for Named Credentials](#)

[Apex Developer Guide: Invoking Callouts Using Apex](#)

[Authentication Provider SSO with Salesforce as the Relying Party](#)

Define a Legacy Named Credential

Create a legacy named credential to specify the URL of a callout endpoint and its required authentication parameters in one definition. You can then specify the legacy named credential as a callout endpoint to let Salesforce handle all authentication. You can also skip remote site settings, which are otherwise required for callouts to external sites, for the site defined in the legacy named credential.

Important: In Winter '23, Salesforce introduced an improved named credential that is extensible and customizable. We strongly recommend that you use this preferred credential instead of legacy named credentials. For information on extensible, customizable named credentials, see [Named Credentials and External Credentials](#). Legacy named credentials are deprecated and will be discontinued in a future release.

Legacy named credentials are supported in these types of callout definitions:

- Apex callouts
- External data sources of these types:
 - Salesforce Connect: OData 2.0
 - Salesforce Connect: OData 4.0
 - Salesforce Connect: Custom (developed with the Apex Connector Framework)
 - Salesforce Connect: Amazon DynamoDB
- External Services

To set up a legacy named credential:

1. From Setup, enter *Named Credentials* in the Quick Find box, then select **Named Credentials**.
2. To create a legacy named credential, click **New Legacy** from the dropdown menu. To edit an existing legacy credential, click its link and click **Edit**.
3. Enter information in the fields.

Field	Description
Label	<p>A user-friendly name for the legacy named credential that's displayed in the Salesforce user interface, such as in list views.</p> <p>If you set <code>Identity Type</code> to Per User, this label appears when your users view or edit their authentication settings for external systems.</p>
Name	<p>A unique identifier that's used to refer to this legacy named credential from callout definitions and through the API.</p> <p>The name can contain only underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.</p>
URL	<p>The URL or root URL of the callout endpoint. Must begin with <code>http://</code> or <code>https://</code>. Can include a path but not a query string. Examples:</p> <ul style="list-style-type: none"> • <code>http://my_endpoint.example.com</code> • <code>https://my_endpoint.example.com/secure/payroll</code>

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions**

USER PERMISSIONS

To view legacy named credentials:

- View Setup and Configuration

To create, edit, or delete legacy named credentials:

- Manage Named Credentials or Customize Applications

Field	Description
	<p>You can, however, append a query string and a specific path in the callout definition's reference to the legacy named credential. For example, an Apex callout could reference the legacy named credential "My_Payroll_System" as follows.</p> <pre>HttpRequest req = new HttpRequest(); req.setEndpoint('callout:My_Payroll_System/paystubs?format=json');</pre>
Certificate	<p>If you specify a certificate, your Salesforce org supplies it when establishing each two-way SSL connection with the external system. The certificate is used for digital signatures, which verify that requests are coming from your Salesforce org.</p> <p>This certificate is for the callout endpoint URL. If you plan to use the JWT or JWT Token Exchange authentication protocol, enter the token endpoint URL certificate in the JWT Signing Certificate field. The JWT Signing Certificate field is displayed when you select <i>JWT</i> or <i>JWT Token Exchange</i> for the Authentication Protocol field, as described in a later step.</p>
Identity Type	<p>Determines whether you're using one set or multiple sets of credentials to access the external system.</p> <ul style="list-style-type: none"> Anonymous: No identity and therefore no authentication. Per User: Use separate credentials for each user who accesses the external system via callouts. Select this option if the external system restricts access on a per-user basis. <p>After you grant user access through permission sets or profiles in Salesforce, users can manage their own authentication settings for external systems in their personal settings. If you're using JWT or JWT Token Exchange, the per-user credentials are handled for them.</p> <ul style="list-style-type: none"> Named Principal: Use the same set of credentials for all users who access the external system from your org. Select this option if you designate one user account on the external system for all your Salesforce org users.

4. Select the authentication protocol.

- If you select **Password Authentication**, enter the username and password for accessing the external system.
- If you select **OAuth 2.0**, complete the following fields.

Field	Description
Authentication Provider	Choose the provider. See Authentication Providers .
Scope	<p>Specifies the scope of permissions to request for the access token. Your authentication provider determines the allowed values. See Use the Scope Parameter.</p> <ul style="list-style-type: none"> The value that you enter replaces the <code>Default Scopes</code> value that's defined in the specified authentication provider. Whether scopes are defined can affect whether each OAuth flow prompts the user with a consent screen. We recommend that you request a refresh token or offline access. Otherwise, when the token expires, you lose access to the external system.

Field	Description
Start Authentication Flow on Save	To authenticate to the external system and obtain an OAuth token, select this checkbox. This authentication process is called an OAuth flow. When you click Save , the external system prompts you to log in. After successful login, the external system grants you an OAuth token for accessing its data from this org. Redo the OAuth flow when you need a new token—for example, if the token expires—or if you edit the <code>Scope</code> or <code>Authentication Provider</code> fields. When the token expires, the external system returns a 401 HTTP error status.

- If you select **JWT** or **JWT Token Exchange**, complete the following fields.

Field	Description
Issuer	Specify who issued the JWT using a case-sensitive string.
Scope	JWT Token Exchange only. Determines the permissions associated with the tokens that you're requesting.
Token Endpoint URL	JWT Token Exchange only. The URL of the authorization provider. JSON Web Token requests are sent to the provider in exchange for access tokens.
Per User Subject	Per User identity type only. Formula string calculating the JWT's subject. Include API names and constant strings in quotes. Allows a dynamic subject unique per user requesting the token. For example, <code>'User='+\$User.Id</code> .
Named Principal Subject	Named Principal identity type only. Enter static text, without quotes, that specifies the JWT subject.
Audiences	External service or other allowed recipients for the JWT. Store each audience as a case-sensitive string on a new line.
Token Valid for	The length of time that the token is valid to authenticate the user into the external system.
JWT Signing Certificate	Certificate verifying the JWT's authenticity to external systems.

- If you select **AWS Signature Version 4**, complete the following fields.

Field	Description
AWS Access Key ID	First part of the access key used to sign programmatic requests to AWS.
AWS Secret Access Key	Second part of the access key used to sign programmatic requests to AWS.
AWS Region	The AWS region name for the legacy named credential's endpoint. For example, <code>us-east-1</code> .
AWS Service	The AWS utility to access.

5. If you want to use custom headers or bodies in the callouts, enable the relevant options.

Field	Description
Generate Authorization Header	<p>By default, Salesforce generates an authorization header and applies it to each callout that references the legacy named credential.</p> <p>Deselect this option only if one of the following statements applies.</p> <ul style="list-style-type: none"> The remote endpoint doesn't support authorization headers. The authorization headers are provided by other means. For example, in Apex callouts, the developer can have the code construct a custom authorization header for each callout. <p>This option is required if you reference the legacy named credential from an external data source.</p>
Allow Merge Fields in HTTP Header	<p>In each Apex callout, the code specifies how the HTTP header and request body are constructed. For example, the Apex code can set the value of a cookie in an authorization header.</p> <p>These options enable the Apex code to use merge fields to populate the HTTP header and request body with org data when the callout is made.</p> <p>These options aren't available if you reference the legacy named credential from an external data source.</p>
Allow Merge Fields in HTTP Body	

To reference a legacy named credential from a callout definition, use the legacy named credential URL. A legacy named credential URL contains the scheme `callout:`, the name of the legacy named credential, and an optional path. For example:

`callout:My_Named_Credential/some_path`.

You can append a query string to a legacy named credential URL. Use a question mark (?) as the separator between the legacy named credential URL and the query string. For example: `callout:My_Named_Credential/some_path?format=json`.

SEE ALSO:

[Legacy Named Credentials](#)

[Authentication Protocols for Named Credentials](#)

[Grant Access to Authentication Settings for Legacy Named Credentials](#)

[Apex Developer Guide : Invoking Callouts Using Apex](#)

[Named Credentials and External Credentials](#)

[User External Credentials](#)

Grant Access to Authentication Settings for Legacy Named Credentials

For legacy named credentials that use per-user authentication, grant access to users through permission sets and profiles. Doing so lets users set up and manage their own authentication settings for accessing the external system.

Important: In Winter '23, Salesforce introduced an improved named credential that is extensible and customizable. We strongly recommend that you use this preferred credential instead of legacy named credentials. For information on extensible, customizable named credentials, see [Named Credentials and External Credentials](#). Legacy named credentials are deprecated and will be discontinued in a future release.

1. From Setup, in the Quick Find box, enter either *Permission Sets* or *Profiles*, and then select either **Permission Sets** or **Profiles**.
2. Click the name of the permission set or profile that you want to modify.
3. Do one of the following.
 - For a permission set, or for a profile in the enhanced profile user interface, click **Named Credential Access** in the Apps section. Then click **Edit**.
 - For a profile in the original profile user interface, click **Edit** in the Enabled Named Credential Access section.
4. Add the legacy named credentials that you want to enable.
5. Save your changes.

SEE ALSO:

[Define a Legacy Named Credential](#)
[Legacy Named Credentials](#)

Authentication Protocols for Named Credentials

Your connections between Salesforce and external systems use an authentication protocol to confirm secure communication between the two systems. Choose the authentication protocol that matches the configuration of the external system that you connect to. When you do, keep the strengths and considerations of each authentication protocol in mind.

Important: In Winter '23, Salesforce introduced an improved named credential that is extensible and customizable. We strongly recommend that you use this preferred credential instead of legacy named credentials. For information on extensible, customizable named credentials, see [Named Credentials and External Credentials](#). Legacy named credentials are deprecated and will be discontinued in a future release.

If you don't want to specify an authentication protocol:

- Select the Custom protocol, and use custom headers for non-legacy named credentials.
- Select **No Authentication** if you're creating a non-legacy or legacy named credential.

AWS Signature Version 4

A protocol to authenticate callouts to resources in Amazon Web Services over HTTP. The identity type must be Named Principal.

If you use the AWS Signature v4 protocol, grant all users Modify All access to user external credentials. See [Enable User External Credentials](#) for more information.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions**

Permission sets available in: **Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To edit permission sets and user profiles:

- **Manage Profiles and Permission Sets**

AWS Signature v4 Variants

Roles Anywhere

Use this variant to request temporary, limited-privilege credentials controlled via IAM policies and roles using a certificate.

IAM User

Use this variant to request temporary, limited-privilege credentials for AWS IAM users.

For an example of how to make a connection using named credentials, AWS Signature Version 4, and STS, see [Define a Named Credential for Salesforce Connect Adapter for Amazon Athena](#).

Custom

A user-created authentication. This authentication protocol isn't available for legacy named credentials.

Specify a permission set, sequence number, and authentication parameters. Each authentication parameter requires a name and value.

JWT

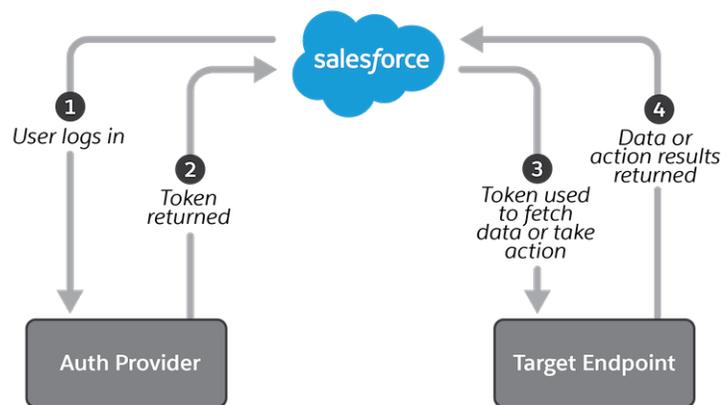
A JWT (rhymes with hot), or JSON Web Token, manages your authentication into the external system.

Users don't manage their credentials for the external system. With this protocol, when users view their authentication settings for external systems, they can't see options.

The subject is a string when the identity type is named principal, and it's a formula when the identity type is per user.

Signing certificates aren't included in packages. If you're using JWT or JWT Bearer Flow as the authentication protocol for a packaged named credential, recreate the package's referenced signing certificate in the subscriber org before installing the package.

OAuth 2.0



A user or the admin applies a credential for a specified OAuth 2.0 system that authenticates into the external system.

OAuth uses an *authentication provider*, which issues a token to Salesforce for calling a target endpoint, after the user logs in via a browser and allows access. To an end user, an authentication provider can appear distinct from the actual target endpoint. For example, a user logs into Google to give an application access to Google Photos or Nest smart home devices. The authentication provider gives Salesforce a “valet key” that it can use for limited access to the user’s resources. For more on OAuth authentication, see [OAuth Authorization Flows](#).

If you’re using OAuth with named principals, grant all users Modify All access to user external credentials. If you’re using OAuth with per-user authentication, grant all users Create, Read, Update, and Delete access to user external credentials. See [Enable User External Credentials](#) for more information.

If you’re using the per-user identity type, each user accessing the external system manages their own credential.

OAuth 2.0 Variants

Browser Flow

One or more users logs into the remote system via a web browser, triggering a callback that includes tokens used to authenticate calls to the endpoint in the Named Credential. Browser Flow is sometimes referred to as Authorization Code Grant Flow.

JWT Bearer Flow

For legacy named credentials, JWT Bearer Flow is referred to as JWT Token Exchange.

A JWT (JSON Web Token) is sent to an authorization provider and receives a token in return that's used to authenticate into the external system.

Users don't manage their credentials for the external system. With this protocol, when users view their authentication settings for external systems, they can't edit options. But users can delete their JWT Bearer Flow settings to use a different named credential.

Signing certificates aren't included in packages. If you're using JWT or JWT Bearer Flow as the authentication protocol for a packaged named credential, recreate the package's referenced signing certificate in the subscriber org before installing the package.

Client Credentials with Client Secret Flow

The client app exchanges its client credentials defined in client identifier and client secret for an access token.

Client Credentials with JWT Assertion

The client app exchanges its client credentials defined client identifier and in JWT assertion for an access token.

Basic

A static username and password are used to directly authenticate into the external system. Basic authentication offers the functionality of the Password protocol with the increased security of permission set assignments. With these permission set assignments, you grant users explicit access to make callouts using a specified set of credentials. This protocol isn't available for legacy named credentials.

With the named principal identity type, a Salesforce admin uses one username and password to authenticate into the external system on behalf of all users. With the per-user identity type, each user accessing the external system manages their own username and password.

Password

This authentication protocol is available only for legacy named credentials. But if you're using the Custom authentication protocol, you can configure a credential that supports the standard HTTP Basic authentication protocol. That protocol uses passwords.

A static username and password are used to directly authenticate into the external system.

If you're using the per-user identity type, each user accessing the external system manages their own username and password.

SEE ALSO:

[Create and Edit an External Credential](#)

[Legacy Named Credentials](#)

[Define a Legacy Named Credential](#)

[Authentication Provider SSO with Salesforce as the Relying Party](#)

Set Up JWT Claims for Named Credentials

External credentials that use JWT authentication have JWT (JSON Web Token) claims. JWT claims assert attributes about tokens, such as time of expiration. You can modify some default claims for an external credential as well as create your own custom claims.

 **Note:** This table doesn't apply to legacy named credentials. For legacy named credentials, see [Define a Legacy Named Credential](#).

Table 15: Default JWT Claims for Named Credentials

Claim Name	Description	Notes
alg	The algorithm used to sign the token. Valid values are RS256 and RS512.	Default is RS256, an asymmetric algorithm that uses a private/public pair.
aud	(Audience) Recipient for whom the token is intended.	Added when claims are edited. Editable through the JWT Claims panel on the editable credential.
exp	(Expiration) Time after which the token expires. Expressed as a <code>NumericDate</code> value, representing the number of seconds from 1970-01-01T00:00:00Z UTC until the specified UTC date/time, ignoring leap seconds.	Set on external credential creation through the Expiration field. If no expiration number is provided, a default of two minutes in the future is set.
iat	(Issued At Time): Time at which the token was issued. Can be used to determine age of the token. Expressed as a <code>NumericDate</code> value, representing the number of seconds from 1970-01-01T00:00:00Z UTC until the specified UTC date/time, ignoring leap seconds.	Added automatically on external credential creation. Not editable.
iss	Issuer of the token. For example, to return the Email ID, use the formula <code>{!\$User.Email}</code> .	Added when claims are edited. Editable through the JWT Claims panel on the editable credential.
kid	(Key ID) Used to match a specific key.	Added automatically on external credential creation. Editable through the JWT Claims panel on the editable credential.
nbf	(Not Before Time) Time before which the token must not be accepted for processing. Expressed as a <code>NumericDate</code> value, representing the number of seconds from 1970-01-01T00:00:00Z UTC until the specified UTC date/time, ignoring leap seconds.	Added automatically on external credential creation. Not editable.
sub	Subject of the token (the user). The subject is a formula, whether the identity type is named principal or per user.	Added when claims are edited. Editable through the JWT Claims panel on the editable credential.
typ	(Type) The media type of the token.	Added automatically on external credential creation. The value is set to 'JWT'. Not editable.

1. On the Named Credentials page, click **External Credential**.
2. Select the external credential you created.
3. Scroll to JWT Claims.
4. Click **Edit**.
5. Optionally, assign a value to these claims: **iss**, **sub**, and **aud**.

You can make a callout without configuring `iss`, `sub`, and `aud`, and your JWT payload won't contain them. However, if you edit any preset claims or add custom claims, you must provide values for all three of these claims.

6. Optionally, modify the value of the **kid** claim. You can also delete this claim.
7. Optionally, add a custom claim of your own. Provide a name, description, and value for the claim, and select either **JWT Body Claim** or **JWT Header Claim** as the type.
8. Save the edited claims.

Congratulations—you've finished the main steps in creating an OAuth external credential. See [Additional Tasks for External Credentials](#) for a few more jobs to complete.

Certificates and Keys

Salesforce certificates and key pairs are used for signatures that verify a request is coming from your organization. They are used for authenticated SSL communications with an external website, or when using your organization as an Identity Provider. You only need to generate a Salesforce certificate and key pair if you're working with an external website that wants verification that a request is coming from a Salesforce organization.

You can export all your certificates and private keys into a keystore for storage or import certificates and keys from a keystore. This keystore lets you move keys from one organization to another. The exported file is in the Java Keystore (JKS) format, and the imported file must also be in the JKS format. For more information about the JKS format, see [Oracle's Java KeyStore documentation](#).

API Client Certificate

The API client certificate is used by workflow outbound messages, the AJAX proxy, and delegated authentication HTTPS callouts. For security reasons, the API client certificate must be known only to your org.

Choose an API client certificate based on the remote endpoint you connect to. Some endpoint servers require a certificate chain that is trusted by a certificate authority; others are fine with directly trusting a self-signed certificate.

[Generate a Self-Signed Certificate](#)

Generate a certificate signed by Salesforce to show that communications purporting to come from your organization are really coming from there.

[Generate a Certificate Signed by a Certificate Authority](#)

A certificate authority-signed (CA-signed) certificate can be a more authoritative way to prove that your org's data communications are genuine. You can generate this type of certificate and upload it to Salesforce.

[Set Up a Mutual Authentication Certificate](#)

To prevent security from being compromised by simple impersonation, you can require clients and servers to prove their identity to each other with a mutual authentication certificate.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions**

USER PERMISSIONS

To create, edit, and manage certificates:

- [Customize Application](#)

[Configure Your API Client to Use Mutual Authentication](#)

Enforce SSL or TLS mutual authentication.

[Manage Master Encryption Keys](#)

Encrypted custom fields, such as `social_security_number` or `credit_card_number`, are encrypted with a master encryption key. This key is automatically assigned when you select fields to encrypt. You manage your own master key according to your organization's security and regulatory needs.

[Replace the Default Proxy Certificate for SAML Single Sign-On](#)

The proxy.salesforce.com default certificate has been retired due to its expiration and for security best practices. If your Salesforce org uses this certificate for SAML single sign-on, act now to prevent a possible interruption of service.

Generate a Self-Signed Certificate

Generate a certificate signed by Salesforce to show that communications purporting to come from your organization are really coming from there.

1. From Setup, search for *Certificate and Key Management* in the Quick Find box.
2. Select **Create Self-Signed Certificate**.
3. Enter a descriptive label for the Salesforce certificate.

This name is used primarily by administrators when viewing certificates.

4. Enter a unique name. You can use the name that's automatically populated based on the certificate label you enter.

This name can contain only underscores and alphanumeric characters, and must be unique in your org. It must begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores. Use the unique name when referring to the certificate using Lightning Platform APIs or Apex.

5. Select a key size for your generated certificate and keys.

Certificates with 2048-bit keys last one year and are faster than certificates with 4096-bit keys. Certificates with 4096-bit keys last two years.



Note: After you save a Salesforce certificate, you can't change its type or key size.

6. Click **Save**.

Downloaded self-signed certificates have `.cert` extensions.

After you successfully save a Salesforce certificate, the certificate and corresponding keys are automatically generated.

You can have a maximum of 50 certificates.



Note: Some business processes require more certificates than others. If you require more than 50 certificates, contact Salesforce Customer Support.

SEE ALSO:

[Certificates and Keys](#)

[Generate a Certificate Signed by a Certificate Authority](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions**

USER PERMISSIONS

To create, edit, and manage certificates:

- Customize Application

Generate a Certificate Signed by a Certificate Authority

A certificate authority-signed (CA-signed) certificate can be a more authoritative way to prove that your org's data communications are genuine. You can generate this type of certificate and upload it to Salesforce.

1. From Setup, enter *Certificate and Key Management* in the Quick Find box, then select **Certificate and Key Management**.

2. Select **Create CA-Signed Certificate**.

3. Enter a descriptive label for the Salesforce certificate.

This name is used primarily by administrators when viewing certificates.

4. Enter a unique name. You can accept the name that's populated based on the certificate label you enter.

This name can contain only underscores and alphanumeric characters, and must be unique in your org. It must begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores. Use the unique name when referring to the certificate using the Lightning Platform API or Apex.

5. Select a key size for your certificate and keys.

For securing data in transit via TLS, we recommend using the default 2048-bit key size. For situations that require stronger keys, such as using Shield Platform Encryption's Bring Your Own Key service, use 4096-bit keys.

 **Note:** After you save a Salesforce certificate, you can't change its type or key size.

6. Enter the following information.

These fields are combined to generate a unique certificate.

Field	Description
Common Name	The fully qualified domain name of the company requesting the signed certificate, generally of the form <code>http://www.mycompany.com</code> .
Email Address	The email address associated with this certificate.
Company	Either the legal name of your company or your legal name.
Department	The branch of your company using the certificate, such as marketing or accounting.
City	The city where the company resides.
State	The state where the company resides.
Country Code	A two-letter code indicating the country where the company resides. For the United States, the value is <i>US</i> .

7. Click **Save**.

After you save a Salesforce certificate, the certificate and corresponding keys are automatically generated.

8. Find your new certificate from the certificates list, then click **Download Certificate Signing Request**.

Downloaded certificate signing requests have `.csr` extensions.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **All Editions**

USER PERMISSIONS

To create, edit, and manage certificates:

- Customize Application

9. Send the certificate request to the certificate authority of your choice.
10. After the certificate authority sends back the signed certificate, go back to *Certificate and Key Management*, click the name of the certificate, then click **Upload Signed Certificate**.
The CA-signed certificate must match the certificate created in Salesforce. If you try to upload a different CA-signed certificate, the upload fails.
11. To complete the upload process, click **Save**.

After you upload the CA-signed certificate, the status of the certificate is changed to Active and you can use it.

 **Tip:** To edit a certificate that you've uploaded, upload it again; published site domains are republished if they have at least one Salesforce Site or Experience Cloud site. The expiration date of the certificate record is updated to the expiration date of the newly uploaded certificate.

You can have up to 50 certificates.

 **Note:** Some business processes require more certificates than others. If you require more than 50 certificates, contact Salesforce Customer Support.

After you create a CA-signed certificate, it's valid for 3 years. After that, the certificate must be renewed, which extends the expiration date.

- If you use the "Serve the domain with the Salesforce Content Delivery Network (CDN)" HTTPS option, Akamai automatically renews the certificate.
- For other HTTPS options, contact your certificate authority (CA) to extend the certificate expiration date.

Set Up a Mutual Authentication Certificate

To prevent security from being compromised by simple impersonation, you can require clients and servers to prove their identity to each other with a mutual authentication certificate.

1. On the Certificate and Key Management page, click **Upload Mutual Authentication Certificate**.

 **Note:** If you don't see this option on the Certificate and Key Management page, contact Salesforce to enable the feature.

2. Give your certificate a label and name, and click **Choose File** to locate the certificate.
3. To finish the upload process, save your changes.
4. Enable the Enforce SSL/TLS Mutual Authentication user permission for an API Only user.
This API Only user configures the API client to connect on port 8443 to present the signed client certificate.

To delete a certificate, from the Certificate and Key Management page in Setup, click **Del** next to the certificate name. If you delete a mutual authentication certificate associated with a user who has the Enforce SSL/TLS Mutual Authentication user permission, it takes up to 5 minutes for the user's session ID to be invalidated and for the certificate to be cleared from the cache.

SEE ALSO:

[Configure Your API Client to Use Mutual Authentication](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Personal, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To create, edit, and manage certificates:

- [Customize Application](#)

Configure Your API Client to Use Mutual Authentication

Enforce SSL or TLS mutual authentication.

For extra security, you can use a certificate chain. A certificate chain is a hierarchical order of certificates where one certificate issues and signs another certificate lower in the hierarchy. Upload a certificate chain as a single PEM-encoded certificate authority-signed (CA-signed) certificate representing the concatenated chain of certificates. The uploaded certificate chain must include the intermediate certificates in this order.

- Start with the server or client certificate, and then add its signing certificate.
- If more than one intermediate certificate exists between the server or client certificate and the root, add each certificate as the one that signed the previous certificate.
- The root certificate is optional, and generally isn't included.

Important: If you're using a certificate chain, the client certificate must include any intermediate certificates in the chain when contacting port 8443. The intermediate certificates must be sent by the client with every request. You can upload either the leaf certificate or the full certificate chain.

Note: If you delete a mutual authentication certificate associated with a user who has the Enforce SSL/TLS Mutual Authentication user permission, it takes up to 5 minutes for the user's session ID to be invalidated and for the certificate to be cleared from the cache.

1. After you set up mutual authentication, log in to the Salesforce service using port 8443 for your My Domain login URL. Include your credentials and your signed certificate information. Your configuration using `cURL` can look something like this example. Replace "`MyDomainName.my.salesforce.com:8443`" with the specific instance's endpoint, replace "`@login.txt`" with your login Soap message credentials, and replace "`fullcert.pem:xxxxxx`" with your certificate information.

```
curl -k https://MyDomainName.my.salesforce.com:8443/services/Soap/u/31.0 -H
"Content-Type: text/xml; charset=UTF-8" -H "SOAPAction: login" -d @login.txt -v -E
fullcert.pem:xxxxxx
```

2. After a session ID is returned from your call, you can perform other actions, such as queries. In this result, `@accountQuery.xml` is the file name containing the query Soap message with the session ID from the login response.

```
curl -k https://MyDomainName.my.salesforce.com:8443/services/Soap/u/31.0 -H
"Content-Type: text/xml; charset=UTF-8" -H "SOAPAction: example" -d @accountQuery.xml
-v -E fullcert.pem:xxxxxx
```

SEE ALSO:

[Certificates and Keys](#)

[Set Up a Mutual Authentication Certificate](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Personal, Unlimited, Developer, and Database.com** Editions

USER PERMISSIONS

To create, edit, and manage certificates:

- Customize Application

To enforce mutual authentication on port 8443 for standard SSL/TLS connections:

(Assign to users with the API Only User permission)

- Enforce SSL/TLS Mutual Authentication

To access Salesforce only through a Salesforce API:

- API Only User

Manage Master Encryption Keys

Encrypted custom fields, such as `social_security_number` or `credit_card_number`, are encrypted with a master encryption key. This key is automatically assigned when you select fields to encrypt. You manage your own master key according to your organization's security and regulatory needs.

 **Note:** Where possible, we changed noninclusive terms to align with our company value of Equality. We maintained certain terms to avoid any effect on customer implementations.

With master encryption keys, you can:

- Archive the existing key and create a new key.
- Export an existing key after it's been archived.
- Delete an existing key.
- Import an existing key after it's been deleted.

 **Note:** This page is about Classic Encryption, not Shield Platform Encryption. [What's the difference?](#)

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions

USER PERMISSIONS

To create, edit, and manage certificates:

- Customize Application

Archiving and Creating New Keys

To archive your current key and create a new key, click **Archive Current Key and Create New Key** on the *Certificate and Key Management* Setup page. A new key is generated, assigned the next sequential number, and activated. All new data is encrypted using the new key.

Existing data continues to use the archived key until the data is modified and saved. Then data is encrypted using the new key.

After you archive a key, you can export or delete it.

Exporting Keys

You can export your keys to a back-up location for safe keeping. It's a good idea to export a copy of any key before deleting it.

Exporting creates a text file with the encrypted key, so you can import the key back into your organization later.

Deleting Keys

Don't delete a key unless you're certain no data is currently encrypted using the key. After you delete a key, any data encrypted with that key can no longer be accessed.

 **Important:** Export and delete keys with care. If your key is destroyed, you must reimport it to access your data. You are solely responsible for making sure your data and keys are backed up and stored in a safe place. Salesforce can't help you with deleted, destroyed, or misplaced keys.

Importing Keys

If you have data associated with a deleted key, you can import an exported key back into your organization. Any data that wasn't accessible becomes accessible again.

Click `Import` next to the key you want to import.

SEE ALSO:

[Certificates and Keys](#)

Replace the Default Proxy Certificate for SAML Single Sign-On

The proxy.salesforce.com default certificate has been retired due to its expiration and for security best practices. If your Salesforce org uses this certificate for SAML single sign-on, act now to prevent a possible interruption of service.

Available in: Both Salesforce Classic and Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited, Developer, and Contact Manager** Editions

Beginning with the Winter '18 release, Salesforce is switching away from the default proxy certificate even if you are still using it. Before the Winter '18 release, manually migrate to a self-signed certificate and update identity providers to prevent an interruption in service. We recommend switching from the default certificate even if your identity provider doesn't validate signatures in SAML requests.

1. If you are using Single SAML Configurations, enable multiple configurations by clicking **Enable Multiple Configs** under Single Sign-On Settings. Read and understand all the instructions on that page. Enabling multiple configurations switches the certificate, so skip Step 2.
2. Edit each affected configuration by changing the Request Signing Certificate to a certificate in your org. If you don't have a certificate and key pair you want to use, upload one or select **Generate self-signed certificate**.
3. Check whether service provider-initiated SAML works properly for your configuration. If it does, no identity provider updates are necessary, and you can skip steps four and five.
If you migrated from a single to multiple configurations, update the Assertion Consumer Service URL.
4. If identity provider updates are necessary, download the certificate you selected for the Request Signing Certificate.
5. Upload this certificate into the identity provider for use in validating SAML requests from Salesforce. If you migrated to multiple configurations from a single configuration, note the Salesforce Login URL and update the value in the identity provider.

Technical Requirements and Performance Best Practices

Review the recommended technical requirements and performance best practices to optimize your Salesforce implementation.

Salesforce provides technical requirements to help you predict whether your hardware and network can provide an acceptable and productive user experience. We strongly recommend testing the actual end-user experience with a configuration identical to what you expect to use in production. Test using the same geographic location, hardware, browser, network settings, and the expected concurrent users for shared hardware like virtual desktops. In Lightning Experience, page load times can be captured using Lightning Component Debug Mode, or by appending `?eptVisible=1` to your URL.

```
https://MyDomainName.lightning.force.com/one/one.app?eptVisible=1
```

Load times are measured in Experienced Page Time, or EPT. EPT measures how long it takes for a page to load so that a user can meaningfully interact with it.

[Technical Requirements for Lightning Experience](#)

The minimum and recommended technical requirements for Lightning Experience.

[Improve Speed and Performance of Lightning Experience Pages](#)

Network, device, browser, and org configuration issues can all affect your Lightning Experience page performance. Learn best practices and common solutions to speed up your system if you're experiencing sluggishness or long page-load times.

Technical Requirements for Lightning Experience

The minimum and recommended technical requirements for Lightning Experience.

For the fastest and most stable experience, we recommend:

- An Octane 2.0 score of 30,000 or greater
- Network latency of 150 ms or less
- Download speed of 3 Mbps or greater
- At least 8 GB of RAM, with 3 GB available for Salesforce browser tabs

Minimum requirements are:

- An Octane 2.0 score of 20,000 or greater
- Network latency of 200 ms or less
- Download speed of 1 Mbps or greater
- At least 5 GB of RAM, with 2 GB available for Salesforce browser tabs

Based on our lab tests, the minimum requirements result in 50% slower page load times and login load times versus the recommended specifications. Users that use over 1,000 records a day are more likely to have their browser tab crash when using the minimum requirements due to memory limits.

You can find your Octane 2.0 score, latency, and download speed by running the Salesforce Performance test. To run the test, append `speedtest.jsp` to your org's domain.

```
https://MyDomainName.lightning.force.com/speedtest.jsp
```

We recommend running this test on the same hardware, network, physical location, and browser as your users. For virtual environments, such as VDI, run all tests from within that virtual environment.

Octane 2.0 is a benchmark developed by Google that measures JavaScript performance. A higher Octane 2.0 score correlates to faster page load times. Octane 2.0 factors in your computer hardware and browser choice.

- Using newer-generation hardware with faster CPUs generates higher Octane 2.0 scores.
- Using the latest version of Salesforce-supported browsers generates higher Octane 2.0 scores.
 - IE11 results in low Octane 2.0 scores and much slower page load speeds.

[Technical Requirements for Phones](#)

The recommended technical requirements for Lightning Experience on phones.

SEE ALSO:

[Improve Speed and Performance of Lightning Experience Pages](#)

[Lightning Console Technical Requirements](#)

[Lightning Reports and Dashboards Technical Requirements](#)

[CRM Analytics Requirements](#)

[Considerations for Installing Data Loader](#)

[Improve Virtual Desktop Environment Performance](#)

Technical Requirements for Phones

The recommended technical requirements for Lightning Experience on phones.

The Salesforce mobile app is available for most Salesforce editions and user license types. The app is supported on various mobile platforms, with some minimum operating system requirements.

Mobile Platform Requirements

The Salesforce mobile app is supported on phones and tablets that meet these mobile platform requirements.

Operating System and Version Requirements

Android 7.0 or later

iOS 14.0 or later

To allow for innovation and to keep Salesforce current in the rapidly evolving mobile market, minimum platform requirements are subject to change at the sole discretion of Salesforce, with or without advance notice.

Mobile Devices Used for Testing

Salesforce performs automated and manual testing of the Salesforce mobile app for iOS and Android on a select set of mobile devices. This is the current list of devices.

Platform	Phones	Tablets
Android	<ul style="list-style-type: none"> • Samsung Galaxy S7 • Samsung Galaxy S8 • Samsung Galaxy S9 / S9+ • Samsung Galaxy Note 9 • Samsung Galaxy S10 / S10e / S10+ • Samsung Galaxy S20 / S20+ • Samsung Galaxy S21 	<ul style="list-style-type: none"> • Samsung Galaxy Tab S6 • Samsung Galaxy Tab S7 • Samsung Galaxy Tab A (8 inch)
iOS	<ul style="list-style-type: none"> • iPhone 8 / 8 Plus • iPhone 11 • iPhone 11 Pro / Pro Max • iPhone 12 • iPhone 12 Pro / Pro Max • iPhone XR • iPhone SE 	<ul style="list-style-type: none"> • iPad Pro (10.5-inch, 11-inch) • iPad Pro (9.7-inch, 6th generation and later) • iPad Air 2 • iPad Mini 4

Customers aren't blocked from using the Salesforce mobile app on untested devices that meet current platform requirements. Salesforce might not be able to replicate some issues for customers using the mobile app on untested devices or due to manufacturer-specific customizations.

 **Note:** Salesforce treats touch-enabled laptops, including Microsoft Surface and Surface Pro devices, as laptops instead of tablets. It's not possible to access the Salesforce mobile app on these devices. Users are always redirected to the full site experience that's

enabled for them—Lightning Experience or Salesforce Classic. Only standard keyboard and mouse inputs are supported on these types of devices.

On phones and older tablet experiences, the Salesforce mobile app is supported in portrait orientation only. On tablets, if using the Lightning on tablet app experience, both portrait and landscape orientations are supported.

Salesforce Editions and Licenses

See which Salesforce editions and user license types support using the Salesforce mobile app.

Salesforce Editions	
<p>Salesforce is available in these editions:</p> <ul style="list-style-type: none"> • Personal Edition • Group Edition • Essentials Edition • Professional Edition • Enterprise Edition • Performance Edition • Unlimited Edition • Developer Edition • Contact Manager Edition 	<p>But not in these editions:</p> <ul style="list-style-type: none"> • Database.com Edition
User License Types	
<p>These user license types can access the Salesforce mobile app. A special mobile license isn't required.</p> <ul style="list-style-type: none"> • Salesforce users • Salesforce Platform and Lightning Platform users • Chatter Plus users (also known as Chatter Only), Chatter Free users, and Chatter External users* • Customer Community, Customer Community Plus, and Partner Community external users • Portal users who are a member of a Salesforce community 	<p>These user license types don't have access to the mobile app:</p> <ul style="list-style-type: none"> • Portal users (unless a member of a Salesforce community) • Database.com users • Sites and Site.com users • Data.com users • WDC users



Note: You can access the same data and functionality that's available to you in the full site, as determined by your organization's Salesforce edition, your user license type, and your assigned user profile and permission sets.

Network

A Wi-Fi® or cellular network connection is required to communicate with Salesforce. For cellular connections, a 3G network or faster is required. For the best performance, we recommend using Wi-Fi or LTE.

In the Salesforce mobile app, you can view your most recently accessed records, and create and edit records, when your device is offline.

Salesforce doesn't provide support or recommend an implementation involving a reverse proxy. Issues that may arise from the use of a reverse proxy and the Salesforce mobile app aren't supported. If customers encounter issues with the app, they must perform due diligence and isolate such issues outside of the reverse proxy integration.

Salesforce Mobile App Updates

Customers whose devices meet current minimum platform requirements are eligible to receive Salesforce mobile app feature updates and fixes.

Our goal is to release Salesforce mobile feature and functionality updates to coincide with each Salesforce major release. This information is provided to help with your release planning, but is subject to change at Salesforce's discretion.

Enhanced features and functionality are provided in major version updates. We aim to release a new major version of the Salesforce mobile app for iOS and Android after the completion of each Salesforce major release to all production instances. The timeframe in which a new major version is released varies and can be affected by factors outside of Salesforce's control, including new requirements from Apple or Google or changes to the iOS or Android operating systems.

Customers can install new major and bug fix versions from the App Store and Google Play as long as their mobile devices meet Salesforce's current minimum mobile operating system requirements. If a device is running an older operating system, updated versions of the Salesforce mobile app don't appear in the App Store or Google Play.

Customer Support Services for Salesforce

Salesforce Customer Support uses commercially reasonable efforts to troubleshoot issues with the Salesforce mobile app, provided:

- A user's device meets current minimum platform requirements
- Users have the most recent version of Salesforce for iOS or Android installed

When customers run the Salesforce mobile app on Salesforce-tested devices, it's more efficient for us to troubleshoot issues. For customers using untested devices, even those meeting minimum platform requirements, we might not be able to replicate some issues due to device manufacturer-specific customizations.

Running the Salesforce mobile app on older devices or devices with low computation and memory capabilities can adversely affect performance, compared to performance on Salesforce-tested devices.

We might not be able to predict or replicate the behavior of beta versions of operating systems, so we support the Salesforce mobile app on generally available (GA) versions of iOS and Android only.

Because we enhance functionality with every release, we support the latest version of the Salesforce mobile app available in the App Store and Google Play only.

SEE ALSO:

[Requirements for the Salesforce Mobile App](#)

Improve Speed and Performance of Lightning Experience Pages

Network, device, browser, and org configuration issues can all affect your Lightning Experience page performance. Learn best practices and common solutions to speed up your system if you're experiencing sluggishness or long page-load times.

The most important factors in predicting page load times are Octane 2.0 score, network latency, download speed, and the amount of customization on a given page.

You can measure your performance by running the Salesforce Performance Test. To run the test, append `speedtest.jsp` to your org's domain.

```
https://MyDomainName.lightning.force.com/speedtest.jsp
```

[Performance Assistant](#)

To ensure that your Salesforce implementation meets your future needs, it's important to develop and test your system with scale in mind. Meet Performance Assistant, your central hub of information and resources about scalability and performance testing with Salesforce. Use the step-by-step instructions, articles, and tools to help you architect your system, conduct performance testing, and interpret your results.

[What Is EPT?](#)

Experienced Page Time (EPT) is a performance metric Salesforce uses in Lightning to measure page load time. EPT measures how long it takes for a page to load into a state that a user can meaningfully interact with.

[Measure Performance for Your Salesforce Org](#)

Set up your test org and test client, and accurately measure performance.

[Network Best Practices](#)

Issues within your network or latency between your device and your Salesforce environment can affect load times.

[Device and Browser Best Practices](#)

To improve device and browser performance, you can take some simple steps. Slow load times can result from devices that don't meet Salesforce minimum technical requirements. Also, plug-ins, extensions, and excessive tabs can consume processing power and memory, degrading performance.

[Org Configuration Best Practices](#)

The way your Salesforce org is configured can lead to slow performance.

[Improve Virtual Desktop Environment Performance](#)

Virtual desktop environments sometimes have older processors and are shared by multiple users, potentially resulting in slower page load times. To predict how a virtual desktop performs with Lightning Experience, run performance tests from within the virtual environment.

SEE ALSO:

[Technical Requirements for Lightning Experience](#)

[Trailhead: Lightning Experience Performance Optimization](#)

[Improve Report Performance](#)

[Improve Dashboard Performance: Best Practices](#)

[Developer Guide: Best Practices for Optimizing Visualforce Performance](#)

[Developer Blog: Lightning Web Components Performance Best Practices](#)

Performance Assistant

To ensure that your Salesforce implementation meets your future needs, it's important to develop and test your system with scale in mind. Meet Performance Assistant, your central hub of information and resources about scalability and performance testing with Salesforce. Use the step-by-step instructions, articles, and tools to help you architect your system, conduct performance testing, and interpret your results.

From Setup, in the Quick Find box, enter *Performance Assistant*, and then select **Performance Assistant**.

We recommend that you integrate performance testing into your release cycle. Performance Assistant guides you through the three main phases of performance testing:

- **Learn:** Learn the basics of scalability and understand the performance testing process from end to end.
- **Prepare:** Create your performance testing strategy, develop a test plan, and schedule your test.
- **Analyze and Optimize:** Interpret your test results, identify performance hotspots, and optimize your solution.

In each phase, Performance Assistant provides guidance and resources to help you test your system with confidence. You can visit Performance Assistant at any time during testing.

EDITIONS

Available in: **Lightning Experience**

Available in: **Professional, Enterprise, Essentials, Unlimited, and Developer Editions**

USER PERMISSIONS

To use Performance Assistant:

- View Setup and Configuration

The screenshot displays the Salesforce Performance Assistant interface. The main content area is titled 'Prepare' and includes a 'Learn' section with a video player and a list of learning resources. A table titled 'Business Scenarios' is visible, showing the following data:

Business Scenarios	Requr
Scenario 1	Result
Scenario 2	20
Scenario 3	30
Scenario 4	40
Scenario 5	50

SEE ALSO:

[Knowledge Article: Performance test FAQs](#)

[Trailblazer Community Group: Salesforce Scalability](#)

What Is EPT?

Experienced Page Time (EPT) is a performance metric Salesforce uses in Lightning to measure page load time. EPT measures how long it takes for a page to load into a state that a user can meaningfully interact with.

A major difference between Salesforce Classic and Lightning Experience is that pages load progressively in Lightning, while pages in Classic are generated on request by the server. Because of the progressive loading from the client, any loaded component in the page can load more components at any time. Measuring when a page finishes loading in Lightning isn't straightforward. Many factors can influence the EPT value.

Client-side and server-side factors both affect EPT. On the client side, the user's browser, hardware, network quality, and their org's complexity all affect EPT. On the server side, Apex and API processing and XMLHttpRequests (XHRs) impact EPT. For instance, component implementation details, errors, caching, and user interactions while the page is loading can all increase EPT.

Other things to consider:

- Lightning UI is rendered client side, making it sensitive to browser performance.
- Lightning UI requires many XHRs to render a page, making it sensitive to network latency.
- Complex pages with many custom fields and components slow page rendering.

The EPT is measured as the time from the page start to when no more activity occurs for at least two frames (~33 ms). The two extra frames help to avoid false positives due to asynchronous calls. These calls include any XHR activity, any storage activity, or any user interaction or client-side work of any kind in the main JavaScript thread.

Measure Performance for Your Salesforce Org

Set up your test org and test client, and accurately measure performance.

A good testing strategy evaluates both performance and scalability. Performance refers to the speed and effectiveness of a system under a given workload within a given time frame. Scalability is the ability of a system to meet its response time or throughput objectives under increasing application and system processing demands. Make your implementation performant and scalable.

[Plan Your Performance Test and Identify Key Personas](#)

Create an accurate sandbox org and plan your test using key personas.

[Set Up and Run Performance Tests](#)

Create tests that evaluate your networks, key personas, and data loading.

SEE ALSO:

[Get Lightning Experience Adoption Insights with the Lightning Usage App](#)

[Get Lightning Experience Adoption Insights from Custom Reports](#)

Plan Your Performance Test and Identify Key Personas

Create an accurate sandbox org and plan your test using key personas.

We recommend using a sandbox that is a full copy of your production org. Make sure that your sandbox's data model is similar to production.

- Draw a system diagram to visualize current and future features, systems, and users that involve Salesforce. For each part of the system, estimate peak load levels, average load levels, and feature use. Consider user arrival rates, login rates, which pages are viewed, and page views per session. If available, any existing site data as a starting point.

- Calculate the throughput of your system in Requests per Second (RPS). RPS combines inbound XMLHttpRequests (XHRs) and API calls, both of which are supported by Event Monitoring. For help with accessing these metrics, see [Using Event Monitoring](#).
 - Estimate the size and shape of your data, including the number of accounts, users, feeds, groups, and other objects.
 - In your sandbox org, include any complex relationships between your objects, role hierarchies, and sharing rules.
-  **Note:** Sandbox and production orgs exist in different instances, have different hardware, and can differ in performance. These differences can be most noticeable in asynchronous processing and database caching. Don't use sandbox performance as a benchmark for production performance. Likewise, don't use production as a benchmark for sandbox performance.

After your sandbox org is set up, identify the key personas for your org and plan your tests around their page flows. Different personas have different data volumes and data visibility. Performance for a persona with a wide view of your org's data, like the VP of Sales, can be different from users with more specialized roles. Use your key personas to build a site map and identify likely page flows for each persona.

Set Up and Run Performance Tests

Create tests that evaluate your networks, key personas, and data loading.

Before measuring your org's performance, measure your browser's octane score and network latency using the same hardware and network conditions as your users. Resolve any performance issues before testing your org.

For each test, define the scope of your investigation, what components are involved in the test, and what metrics you want to measure. Run your performance test multiple times to eliminate variance. Run your tests at regular intervals, and take note of any changes in response times and throughput. Performance testing is an iterative process. Finding and solving issues uncovered by your tests can uncover more issues.

-  **Note:** For step-by-step guidance on designing, executing, and analyzing performance tests, use Performance Assistant. For more information, see [Performance Assistant](#).

Salesforce measures performance in Experienced Page Time (EPT). You can measure EPT in four ways.

Add an EPT counter to the header of your app

To add an EPT counter to the header of your app, use Lightning Component Debug Mode, or append `?eptVisible=1` to your URL.

```
https://MyDomainName.lightning.force.com/one/one.app?eptVisible=1
```

Lightning Component Debug Mode slows performance because it doesn't minify code. Using `?eptVisible=1` has a smaller impact on performance.

Use the Lightning Usage App to view page and browser performance

To measure EPT with the Lightning Usage App, select a tab in the Activity or Usage section on the left side of the page. You can view EPT by the browser used, or by page. Because the Lightning Usage App aggregates performance metrics, using the EPT counter can be better for measuring specific pages.

Build a custom report using Lightning Usage App objects

To measure EPT with custom reports in the Lightning Usage App, create a report type using a Lightning Usage App object. After you create the report type, build the report using Report Builder. Available Lightning Usage App objects are:

- LightningUsageByAppTypeMetrics
- LightningUsageByBrowserMetrics
- LightningUsageByPageMetrics
- LightningUsageByFlexiPageMetrics

Use the Event Monitoring Analytics App to monitor performance with event types

To measure EPT with the Event Monitoring Analytics App, use the prebuilt Lightning Performance dashboard. You can also use event types to monitor specific aspects of performance. Some useful event types include:

- Apex REST API
- Lightning Page View
- Lightning Error
- Lightning Interaction
- Lightning Performance

In addition to EPT, use browser developer tools to test network throttling, and use automation tools such as Selenium to test page flow performance. Write persona-based load generation scripts using tools such as LoadRunner or JMeter.

Example:

- In a single user performance test, you can look at a Lightning page with custom components. For that test, measure EPT, octane score, and network performance.
- In a large data volume test, you can look at a list view with many records and complex filters. For that test, focus on SOQL performance.
- When testing API performance, you can look at Account object updates using the SOAP API. For that test, measure request throughput and database time.

SEE ALSO:

[Trailhead: Measure Lightning Experience Performance and Experienced Page Time \(EPT\)](#)

[Event Monitoring Analytics App](#)

[Event Monitoring Analytics App Prebuilt Dashboards](#)

[Developer Guide: EventLogFile Supported Event Types](#)

[Developer Blog: Open Sourcing Performance Metrics Gathering for Salesforce Platform](#)

[Developer Guide: Salesforce Lightning Inspector Chrome Extension](#)

Network Best Practices

Issues within your network or latency between your device and your Salesforce environment can affect load times.

Accessing a host instance from a different geographical location can lead to slow performance. You can find your Salesforce org's instance listed under the Your Server field in the Salesforce Performance Test.

Latency issues between the client device and remotely located web servers or issues within your network can cause degraded performance. Virtual private networks that require routing through a corporate office or data center before rerouting to a Salesforce org can increase latency. Ask your company's network admin or IT professionals to assess your network latency when connecting to your Salesforce environment.

Enable CDN to Load Lightning Experience Faster

A content delivery network (CDN) improves the load time of static content by storing cached versions in multiple geographic locations. There's a checkbox in Session Settings in Setup to enable Lightning Experience to leverage Akamai's CDN and thus reduce page load

times for your users. When the CDN is enabled, it turns on CDN delivery for the static JavaScript and CSS in the Lightning Component framework that powers Lightning Experience. It doesn't distribute your Salesforce data or metadata in a CDN.

SEE ALSO:

[Knowledge Article: Troubleshoot network performance issues with ping and traceroute](#)

[Modify Session Security Settings](#)

Device and Browser Best Practices

To improve device and browser performance, you can take some simple steps. Slow load times can result from devices that don't meet Salesforce minimum technical requirements. Also, plug-ins, extensions, and excessive tabs can consume processing power and memory, degrading performance.

If your device shows poor performance, try these steps:

- Make sure that your device is fully charged or connected to power. Devices on low battery tend to run at lower speeds to conserve power.
- Close other applications.
- Disable or remove unused or unnecessary browser plug-ins and extensions.
- Use the latest stable version of your browser.
- Switch to a different browser. Chrome is generally the fastest browser for Lightning Experience, while Internet Explorer is generally the slowest.
- Reset browser settings to the default settings.
- Restart your device or browser.
- Upgrade your device to a model with higher specifications.

Org Configuration Best Practices

The way your Salesforce org is configured can lead to slow performance.

Unoptimized Visualforce implementations can impact performance on Visualforce pages. Follow Visualforce best practices outlined in this [developer guide](#).

Some orgs have Lightning Component debug mode enabled for certain users. Lightning Component debug mode negatively affects performance. Enable debug mode only for users actively debugging Lightning components.

Pages with many fields, inefficient custom components, or complex page configurations, can have long load times. To improve performance, consider simplifying those pages. Try these tips to get started:

- To get recommendations for feature improvement, clean up customizations, reduce complexity, and drive feature adoption, try running Salesforce Optimizer first.
- Use profiles to streamline the number of fields. Configure the page so that only the most relevant fields initially display for the user.
- Break page elements like fields, related lists, and custom components into different tabs. Display the most relevant information on the first tab, and move other information to other tabs. Components outside of the primary tab are rendered on demand, not in the initial page load.
- Move the Details component to a secondary tab, or reduce the number of fields displayed.
- Move the Related Lists component to a secondary tab, or use the Related List (singular) component instead. Try to keep the number of related lists to three or fewer.

- Test and refactor any inefficient custom components. See if you can replace any custom components with Lightning Actions. If you have to use custom components, follow the Lightning component best practices outlined in this [developer blog](#).
- Consider using console navigation. Console navigation is a tab-based workspace that can perform faster for certain user flows, particularly in multitasking.

SEE ALSO:

[Developer Guide: Enable Debug Mode for Lightning Components](#)

[Improve Your Implementation with Salesforce Optimizer](#)

[Salesforce Console in Lightning Experience](#)

Improve Virtual Desktop Environment Performance

Virtual desktop environments sometimes have older processors and are shared by multiple users, potentially resulting in slower page load times. To predict how a virtual desktop performs with Lightning Experience, run performance tests from within the virtual environment.

When testing your virtual desktop environment, use as many concurrent users as expected in production, and take their usage patterns into account. Run `speedtest.jsp` to determine the Octane 2.0 score during concurrent use, and test page load times during concurrent use using Lightning Component Debug Mode or the `epTVisible=1` URL parameter.

If your Octane 2.0 score is below 20,000, or you have slow page load times, Salesforce recommends upgrading your hardware, reducing the number of users per environment, or using dedicated desktops.

SEE ALSO:

[Technical Requirements for Lightning Experience](#)

Monitor Your Organization

Salesforce provides a variety of ways to keep tabs on activity in your Salesforce organization so you can make sure you're moving in the right direction.

[The System Overview Page](#)

The system overview page shows usage data and limits for your organization, and displays messages when you reach 95% of your limit (75% of portal roles).

[Monitor Data and Storage Resources](#)

View your Salesforce org's storage limits and usage from the Storage Usage page in Setup.

[Get Adoption and Security Insights for Your Organization](#)

The Lightning Usage App lets you monitor adoption and usage of Lightning Experience in your org, with metrics such as daily active Lightning Experience users and the most visited pages in Lightning Experience. In addition, the app lets you monitor login metrics in your org. See how many users are logging in with your org's various identity services, including Multi-Factor Authentication (MFA) and Single Sign-On (SSO).

[Monitor Login Activity with Login Forensics](#)

Login forensics helps administrators better determine which user behavior is legitimate to prevent identity fraud in Salesforce.

[Manage Real-Time Event Monitoring Events](#)

Manage streaming and storage settings for Real-Time Event Monitoring events declaratively with the Event Manager. You can also manage settings programmatically with the Metadata API. Real-Time Event Monitoring helps you monitor and detect standard events in Salesforce in near real-time. You can store the event data for auditing or reporting purposes. You can create transaction security policies using Condition Builder—a point-and-click tool—or Apex code.

[Monitor Training History](#)

As an administrator, you want to know that your team is learning how to use Salesforce effectively. The Training Class History shows you all of the Salesforce training classes your users have taken.

[Monitor Setup Changes with Setup Audit Trail](#)

Setup Audit Trail tracks the recent setup changes that you and other admins make. Audit history is especially useful when there are multiple admins.

[Field History Tracking](#)

You can select certain fields to track and display the field history in the History related list of an object. When Field Audit Trail isn't enabled, field history data is retained for up to 18 months, and up to 24 months via the API. If Field Audit Trail is enabled, field history data is retained until manually deleted. You can manually delete field history data at any time. Field history tracking data doesn't count against your data storage limits.

[Monitor Debug Logs](#)

Set trace flags to trigger logging for users, Apex classes, and Apex triggers in the Developer Console or in Setup. Monitor the resulting logs to diagnose problems in your org.

[Monitoring Scheduled Jobs](#)

The All Scheduled Jobs page lists all reporting snapshots, scheduled Apex jobs, and dashboards scheduled to refresh.

[Monitor Background Jobs](#)

You can monitor background jobs in your organization, such as when parallel sharing recalculation is running.

[Manage Bulk Data Load Jobs](#)

You can create update, or delete a large volume of records with the Bulk API, which is optimized for processing large sets of data. It makes it simple to load, update, or delete data from a few thousand to millions of records.

The System Overview Page

The system overview page shows usage data and limits for your organization, and displays messages when you reach 95% of your limit (75% of portal roles).

 **Note:** The system overview page shows only the items enabled for your org. For example, your system overview page shows workflow rules only if workflow is enabled for your org.

Click the numbers under each metric to get more details about your usage. If it's available, use Checkout to increase usage limits for your org. For example, if your org reaches the limit for custom objects, the system overview page notifies you with a message link. Click the link to clean up any unused objects, or visit Checkout to increase your limit for objects.

To access the system overview page, from Setup, enter *System Overview* in the Quick Find box, then select **System Overview**.

The system overview page displays usage for:

- Schema
- API usage
- Business logic

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: All Editions except **Personal** Edition

USER PERMISSIONS

To access the system overview page:

- Customize Application

- User interface
- Most used licenses
- Portal roles

 **Note:** The object limit percentages are truncated, not rounded. For example, if your org uses 95.55% of the limit for a particular customization, the object limit displays 95%.

System Overview: Schema

The Schema box in the system overview page shows usage information for custom objects, custom settings, custom metadata types, and data storage.

System Overview: API Usage

The API Usage box in the system overview page shows usage information for API requests in the last 24 hours.

System Overview: Business Logic

The Business Logic box on the system overview page shows usage information for rules, Apex triggers, Apex classes, and code used.

System Overview: User Interface

The User Interface box in the system overview page shows usage information for custom apps, published Site.com sites, active Salesforce sites, active flows, custom tabs, and Visualforce pages.

System Overview: Most Used Licenses

The Most Used Licenses box in the system overview page counts only active licenses, and by default shows the top three used licenses for your org. Any license that reaches 95% usage also appears.

System Overview: Portal Roles

The Portal Roles box in the system overview page shows the usage data and limit for total partner portal, Customer Portal, and Communities roles. The system overview page displays a message when your org reaches 95% of its allotted portal roles.

System Overview: Schema

The Schema box in the system overview page shows usage information for custom objects, custom settings, custom metadata types, and data storage.

- Your Custom Objects + Your Custom Settings—Quantity of active custom objects and settings created by you and users in your org.
- Total Custom Objects + Total Custom Settings—Quantity of active and inactive objects in your org, including the objects created by you, created by users, or installed from packages. This number includes soft-deleted custom objects that are still waiting to be hard deleted. We recommend that you hard delete or erase custom objects you no longer need.

 **Note:** Compare the number of custom objects and settings that you created against the total number in your org, including the ones installed from packages. These values help you understand how many custom objects you can still create or install before you reach the limit.

- Custom Metadata Types—Quantity of visible and hidden custom metadata types used. This count includes all custom metadata types regardless of their visibility setting or how they were installed. All custom metadata types installed from packages appear in this count. Use this page to determine whether your org is close to the limit.
- Custom Metadata Type Usage—Size of custom metadata type records used.
- Data Storage—Quantity of total bytes used.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: all editions except **Personal** Edition

System Overview: API Usage

The API Usage box in the system overview page shows usage information for API requests in the last 24 hours.

Limits are enforced against the aggregate of all API calls made to the org in a 24-hour period. Limits aren't on a per-user basis. When an org exceeds a limit, all users in the org can be temporarily blocked from making additional calls. Calls are blocked until usage for the preceding 24 hours drops below the limit.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

System Overview: Business Logic

The Business Logic box on the system overview page shows usage information for rules, Apex triggers, Apex classes, and code used.

The Code Used section represents the total number of characters in your Apex triggers and Apex classes (excluding comments, test methods, and `@isTest` annotated classes).

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

System Overview: User Interface

The User Interface box in the system overview page shows usage information for custom apps, published Site.com sites, active Salesforce sites, active flows, custom tabs, and Visualforce pages.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: All Editions except **Personal** Database.com

System Overview: Most Used Licenses

The Most Used Licenses box in the system overview page counts only active licenses, and by default shows the top three used licenses for your org. Any license that reaches 95% usage also appears.

Click **Show All** to view all the licenses for your org.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: All Editions except **Personal** Edition

System Overview: Portal Roles

The Portal Roles box in the system overview page shows the usage data and limit for total partner portal, Customer Portal, and Communities roles. The system overview page displays a message when your org reaches 95% of its allotted portal roles.

The default number of roles used in an org's portals or communities is 50,000. This limit includes roles associated with all of the org's customer portals, partner portals, or communities. To prevent unnecessary growth of this number, we recommend reviewing and reducing the number of roles. If you're expecting a high-volume of users, we recommend that you enable account role optimization (ARO). It works by delaying the account role creation process until there's a second user and roles become necessary to support sharing data between them. You can also delete unused roles.

Contact customer support to increase your number of roles. If you require 100,000 roles or more, contact your Salesforce account representative.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

Monitor Data and Storage Resources

View your Salesforce org's storage limits and usage from the Storage Usage page in Setup.

Storage is divided into two categories. File storage includes files in attachments, Files home, Salesforce CRM Content, Chatter files (including user photos), the Documents tab, the custom File field on Knowledge articles, and Site.com assets. Data storage includes the following:

- Accounts
- Action Cadence
- Action Cadence Rule
- Action Cadence Rule Condition
- Action Cadence Step
- Action Cadence Step Tracker
- Action Cadence Step Variant
- Action Cadence Tracker
- Action Cadence Step Monthly Metric
- Article types (format: "[*Article Type Name*]")
- Article type translations (format: "[*Article Type Name*] Version")
- Campaigns
- Campaign Members

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **All** Editions

USER PERMISSIONS

To view storage usage:

- Manage Internal Users
- AND
- Manage Users

- Cases
- Case Teams
- Contacts
- Contracts
- Custom objects
- Data translations
- Email messages
- Events
- Flow Interviews
- Forecast items
- Google docs
- Ideas
- Leads
- List Email
- Notes
- Opportunities
- Opportunity Splits
- Orders
- Quotes
- Quote Template Rich Text Data
- Solutions
- Tags: Unique tags
- Tasks
- All objects tied to Field Service enablement (for a full list, see the [Field Service Developer Guide](#))

Data Storage

Starting in late March 2019, Contact Manager, Group, Essentials, Professional, Enterprise, Performance, and Unlimited Editions are allocated 10 GB for data storage, plus incrementally added user storage. Starter Edition is allocated 10 GB for data storage, plus incrementally added user storage. For example, a Professional Edition org with 10 users receives 10 GB of data storage, plus 200 MB, for 10.2 GB of total data storage.

File Storage

Contact Manager, Group, Professional, Enterprise, Performance, and Unlimited Editions are allocated 10 GB of file storage per org. Essentials and Starter Editions are allocated 1 GB of file storage per org.

Orgs are allocated additional file storage based on the number of standard user licenses. In Enterprise, Performance, and Unlimited Editions, orgs are allocated 2 GB of file storage per user license. Contact Manager, Group, Professional Edition orgs are allocated 612 MB per standard user license, which includes 100 MB per user license plus 512 MB per license for the Salesforce CRM Content feature license. An org with fewer than 10 users will receive a total of 1 GB of per-user file storage rather than 100 MB per user license.

Each Salesforce CRM Content feature license provides an additional 512 MB of file storage, whether Salesforce CRM Content is enabled or not.

File storage and data storage are calculated asynchronously, so if you import or add a large number of records or files, the change in your org's storage usage isn't reflected immediately.

The minimum values apply to Salesforce and Salesforce Platform user licenses. If your org uses custom user licenses, contact Salesforce to determine your exact storage amount.

Big Object Storage

Contact Manager, Group, Enterprise, Performance, Unlimited, Developer, and Personal editions are allocated storage for 1 million big object records per org. Contact Salesforce to increase the limit. Big object storage is calculated asynchronously, so new records aren't immediately reflected. While big object record limits are not actively monitored, Salesforce reserves the right to enforce the limit if necessary. In most cases, the allocation is enforced and records can't be added once the allocation is exceeded. For active production orgs, the allocation of big object records is enforced contractually.

Salesforce Edition	Data Storage Minimum per Org	Data Storage Allocation per User License	File Storage Allocation per Org	File Storage Allocation per User License
Contact Manager				
Group		20 MB		612 MB
Professional				
Enterprise	10 GB		10 GB	
Performance		120 MB		
Unlimited		20 MB for Lightning Platform Starter user licenses		2 GB
Developer	5 MB			
Personal	20 MB (approximately 10,000 records)	N/A	20 MB	N/A
Essentials	10 GB		1 GB	
Starter	10 GB		1 GB	

The values in the File Storage Allocation Per User License column apply to Salesforce and Salesforce Platform user licenses.

 **Note:** Under Current File Storage Usage, the values in the Percent column represent the percentage of storage in use rather than of all storage available. So, let's say there's one photo file in storage and no other file types. The Percent value for that one photo file is 100%. Our one photo file is using all the file storage currently in use. Add more files of different types, and the percentage is recalculated.

Notice in this illustration how the Percent values for Photos and Content Bodies add up to 100%. Though the file sizes add up to only 475 KB, these files represent 100% of the files currently using storage.

Record Type	Record Count	Storage	Percent
Photos	14	129 KB	27%
Content Bodies	3	346 KB	73%

If your org uses custom user licenses, contact Salesforce to determine if these licenses provide more storage.

View Storage Usage

To view your org's current storage usage from Setup, enter *Storage Usage* in the *Quick Find* box, then select **Storage Usage**. You can view the available space for data storage and file storage, the amount of storage in use per record type, the top users according to storage utilization, and the largest files in order of size. To view what types of data a particular user is storing, click that user's name.

In all Editions except Personal Edition, administrators can view storage usage on a user-by-user basis.

1. From Setup, enter *Users* in the *Quick Find* box, then select **Users**.
2. Click the name of any user.
3. Click **View** next to the *Used Data Space* or *Used File Space* fields to view that user's storage usage by record type.

Data storage and file storage are calculated asynchronously and your org's storage usage isn't updated immediately. Keep this in mind if importing or adding many records or files.

Individual users can view their own storage usage in their personal information.

Increase Storage

When you need more storage, increase your storage limit or reduce your storage usage.

- Purchase more storage space, or add user licenses in Professional, Enterprise, Unlimited, and Performance Editions.
- Delete outdated leads or contacts.
- Remove any unnecessary attachments.
- Delete files in Salesforce CRM Content.

Storage Considerations

When planning your storage needs, keep in mind:

- Person accounts count against both account and contact storage because each person account consists of one account as well as one contact.
- Archived activities count against storage.
- Active or archived products, price books, price book entries, and assets don't count against storage.

Get Adoption and Security Insights for Your Organization

The Lightning Usage App lets you monitor adoption and usage of Lightning Experience in your org, with metrics such as daily active Lightning Experience users and the most visited pages in Lightning Experience. In addition, the app lets you monitor login metrics in your org. See how many users are logging in with your org's various identity services, including Multi-Factor Authentication (MFA) and Single Sign-On (SSO).

SEE ALSO:

[Get Lightning Experience Adoption Insights with the Lightning Usage App](#)

[Get Lightning Experience Adoption Insights from Custom Reports](#)

Monitor Login Activity with Login Forensics

Login forensics helps administrators better determine which user behavior is legitimate to prevent identity fraud in Salesforce.

Companies continue to view identity fraud as a major concern. Given the number of logins to an org on a daily—even hourly—basis, it can be a challenge for security practitioners to determine if a specific user account is compromised.

Login forensics helps you identify suspicious login activity. It provides you key user access data, including:

- The average number of logins per user per a specified time period
- Who logged in more than the average number of times
- Who logged in during non-business hours
- Who logged in using suspicious IP ranges

There's some basic terminology to master before using this feature.

Event

Anything that happens in Salesforce, including user clicks, record state changes, and taking measurements of various values. Events are immutable and timestamped.

Login Event

A single instance of a user logging in to an organization. Login events are similar to login history in Salesforce. However, you can add HTTP header information to login events, which makes them extensible.

Login History

The login history that administrators can obtain by downloading the information to a `.csv` or `.gzip` file and the login history that's available through Setup and the API. This data has indexing and history limitations.

Administrators can track events using the `LoginEvent` object. There's no user interface for login forensics. To interact with this feature, use the Salesforce Extensions for Visual Studio Code, Postman, or other development tools.

[Considerations for Using Login Forensics](#)

Before you get started with login forensics, keep these considerations in mind.

[Enable Login Forensics](#)

Perform this quick, one-time setup to start collecting data about your org's login events.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

Enable Login Forensics

Perform this quick, one-time setup to start collecting data about your org's login events.

1. From Setup, in the Quick Find box, enter *Event Manager*, and select **Event Manager**.
2. Click the dropdown next to Login Event, and select **Enable Storing**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise, Unlimited, and Developer** Editions

Requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions.

USER PERMISSIONS

To enable login forensics:

- View Real-Time Event Monitoring Data AND API Enabled

Manage Real-Time Event Monitoring Events

Manage streaming and storage settings for Real-Time Event Monitoring events declaratively with the Event Manager. You can also manage settings programmatically with the Metadata API. Real-Time Event Monitoring helps you monitor and detect standard events in Salesforce in near real-time. You can store the event data for auditing or reporting purposes. You can create transaction security policies using Condition Builder—a point-and-click tool—or Apex code.

 **Important:** Viewing Real-Time Event Monitoring events requires Salesforce Shield or Salesforce Event Monitoring add-on subscriptions. You don't need this add-on to view streaming logout events.

 **Note:** Real-Time Event Monitoring objects sometimes contain sensitive data. Assign object permissions to Real-Time Events accordingly in profiles or permission sets.

1. From Setup, in the Quick Find box, enter *Events*, then select **Event Manager**.
2. Next to the event you want to enable or disable streaming for, click the dropdown menu.
3. Select whether you want to enable or disable streaming or storing on the event.

SEE ALSO:

[Real-Time Event Monitoring](#)

[Stream and Store Event Data](#)

[Metadata API Developer Guide: RealTimeEventSettings](#)

USER PERMISSIONS

To update events in Event Manager:

- Customize Application AND View Setup

Monitor Training History

As an administrator, you want to know that your team is learning how to use Salesforce effectively. The Training Class History shows you all of the Salesforce training classes your users have taken.

Administrators can view the Training Class History from Setup by entering *Training History* in the **Quick Find** box, then selecting **Training History**. After taking a live training class, users must submit the online training feedback form to have their training attendance recorded in the training history.



Note: If you don't see this link under **Manage Users**, your organization has been migrated to a new system. You need to be a Help & Training Admin to access the training reports via My Cases in Help & Training. Contact Salesforce if you do not have this access.

Monitor Setup Changes with Setup Audit Trail

Setup Audit Trail tracks the recent setup changes that you and other admins make. Audit history is especially useful when there are multiple admins.

1. From Setup, in the Quick Find box, enter *View Setup Audit Trail*, and then select **View Setup Audit Trail**.

The history shows the 20 most recent setup changes made to your org. It lists the date of the change, who made it, and what the change was. If a delegate such as an admin or customer support representative makes a setup change on behalf of an end user, the Delegate User column shows the delegate's username. For example, if a user grants login access to an admin and the admin makes a setup change, the admin's username is listed in the Delegate User column. The user granting access is listed in the User column.

2. To download your org's complete setup history for the past 180 days, click **Download**.

After 180 days, setup entity records are deleted.

Changes tracked by the Setup Audit Trail include:

Setup	Changes Tracked
Administration	<ul style="list-style-type: none"> • Company information, default settings like language or locale, and company messages • Multiple currencies • Users, portal users, roles, permission sets, and profiles • Email addresses for any user • Deleting email attachments sent as links • Email footers, including creating, editing, or deleting • Email deliverability settings

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Group, Essentials, Professional, Enterprise, Performance, Unlimited**, and **Database.com** Editions

USER PERMISSIONS

To view training history:

- Manage Users

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Contact Manager, Essentials, Group, Professional, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

USER PERMISSIONS

To view audit trail history:

- View Setup and Configuration

Setup	Changes Tracked
	<ul style="list-style-type: none"> • Divisions, including creating, editing, and transferring and changing users' default division • Certificates, adding or deleting • My Domain settings and changes • Enabling or disabling Salesforce as an identity provider • DKIM, email relay, and email domain filter values when a record is created, edited, or deleted
Profiles	<ul style="list-style-type: none"> • Permission for a standard or custom profile changed • General or admin permission changed • FLS changed on the profile • Entity permission for a standard or custom profile changed • Profile Page Layout changed • Tab set on a standard or custom profile changed • User tab set override changed • User tab set customization override changed for standard or custom profiles • Tab set visibility changed for a standard or custom profile • Tab set visibility modified • Default tab set modified • Custom App default changed on standard or custom profiles • Profile renamed, cloned, or deleted • Profile description changed • Standard or custom profile cloned • Console setting or layout changed • View, or modify, all data enabled for this profile • Login hours for the profile modified. • Client settings for the profile modified • Record type added to or removed from the profile • Default record type modified • Default person account record type modified • Default business account record type modified • Single sign on enabled or disabled for this profile
Permission Sets/Groups	<ul style="list-style-type: none"> • Permission set (or group) created, cloned, or deleted • Permission set (or group) assigned or removed for a user • Permission set (or group) changes to the assignment expiration date (beta) • Permission set created or cloned without a license • Developer name, label, or description of a permission set changed • Session activation changed by admin • Permission in a permission set enabled or disabled by admin • FLS for an object in a permission set changed by admin

Setup	Changes Tracked
	<ul style="list-style-type: none"> • Permission set from a user assigned or unassigned by admin • Tab settings in a permission set changed by admin • Permission set group recalculated
Customization	<ul style="list-style-type: none"> • User interface settings like collapsible sections, Quick Create, hover details, or related list hover links • Page layout, action layout, and search layouts • Compact layouts • Salesforce app navigation menu • Inline edits • Custom fields and field-level security, including formulas, picklist values, and field attributes like the auto-number field format, field manageability, or masking of encrypted fields • Lead settings, lead assignment rules, and lead queues • Activity settings • Support settings, case assignment and escalation rules, and case queues • Requests to Salesforce Customer Support • Tab names, including tabs that you reset to the original tab name • Custom apps (including Salesforce console apps), custom objects, and custom tabs • Contract settings • Forecast settings • Email-to-Case or On-Demand Email-to-Case, enabling or disabling • Custom buttons, links, and s-controls, including standard button overrides • Drag-and-drop scheduling, enabling or disabling • Similar opportunities, enabling, disabling, or customizing • Quotes, enabling or disabling • Data category groups, data categories, and category-group assignments to objects • Article types • Category groups and categories • Salesforce Knowledge settings • Ideas settings • Answers settings • Field tracking in feeds • Campaign influence settings • Critical updates, activating or deactivating • Chatter email notifications, enabling or disabling • Chatter new user creation settings for invitations and email domains, enabling or disabling • Validation rules
Security and Sharing	<ul style="list-style-type: none"> • Public groups, sharing rules, and org-wide sharing, including the Grant Access Using Hierarchies option • Password policies

Setup	Changes Tracked
	<ul style="list-style-type: none"> • Password resets • Session settings, like session timeout (excluding Session times out after and Session security level required at login profile settings) • Delegated administration groups and the items delegated admins can manage (setup changes made by delegated administrators are also tracked) • Lightning Login, enabling or disabling, enrollments, and cancellations • How many records a user permanently deleted from their Recycle Bin and from the Org Recycle Bin • SAML (Security Assertion Markup Language) configuration settings • Salesforce certificates • Identity providers, enabling or disabling • Named credentials • Service providers • Shield Platform Encryption setup • Event Manager • Transaction Security • Some connected app policy and setting updates
Data Management	<ul style="list-style-type: none"> • Using mass delete, including when a mass delete exceeds the user's Recycle Bin limit on deleted records • Data export requests • Mass transfer use • Reporting snapshots, including defining, deleting, or changing the source report or target object on a reporting snapshot • Use of the Data Import Wizard • Sandbox deletions
Development	<ul style="list-style-type: none"> • Apex classes and triggers • Visualforce pages, custom components, and static resources • Lightning components • Lightning pages • Action link templates • Custom settings • Custom metadata types and records • Remote access definitions • Salesforce Sites settings • Platform event channels and channel members, and enriched fields
Various Setups	<ul style="list-style-type: none"> • API usage metering notification, creating • Territories • Process automation settings

Setup	Changes Tracked
	<ul style="list-style-type: none"> • Approval processes • Workflow actions, creating or deleting • Flows • Packages from Salesforce AppExchange that you installed or uninstalled • Notification delivery settings for custom and standard notification types
Using the application	<ul style="list-style-type: none"> • Account team and opportunity team selling settings • Activating Google Apps services • Mobile configuration settings, including data sets, mobile views, and excluded fields • Users with the “Manage External Users” permission logging in to the partner portal as partner users • Users with the “Manage Customer Users” permission logging in to the Salesforce Customer Portal as Customer Portal users • Partner portal accounts, enabling or disabling • Salesforce Customer Portal accounts, disabling • Salesforce Customer Portal, enabling or disabling • Creating multiple Customer Portals • Entitlement processes and entitlement templates, changing or creating • Self-registration for a Salesforce Customer Portal, enabling or disabling • Customer Portal or partner portal users, enabling or disabling

SEE ALSO:

[Security Health Check](#)

Field History Tracking

You can select certain fields to track and display the field history in the History related list of an object. When Field Audit Trail isn't enabled, field history data is retained for up to 18 months, and up to 24 months via the API. If Field Audit Trail is enabled, field history data is retained until manually deleted. You can manually delete field history data at any time. Field history tracking data doesn't count against your data storage limits.

You can track the field history of custom objects and the following standard objects.

- Accounts
- Articles
- Assets
- Campaigns
- Cases
- Contacts
- Contracts
- Contract Line Items

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)), Lightning Experience, and the Salesforce app

Available in: **Contact Manager, Essentials, Group, Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

Standard Objects aren't available in **Database.com**

- Crisis
- Employees
- Employee Crisis Assessments
- Entitlements
- Events
- Individuals
- Internal Organization Units
- Knowledge
- Leads
- Opportunities
- Orders
- Order Products
- Products
- Price Book Entries
- Quote
- Quote Line Item
- Service Appointments
- Service Contracts
- Service Resources
- Solutions
- Tasks
- Work Orders
- Work Order Line Items

Modifying any of these fields adds an entry to the History related list. All entries include the date, time, nature of the change, and who made the change. Not all field types are available for historical trend reporting. Certain changes, such as case escalations, are always tracked.

Salesforce stores an object's tracked field history in an associated object called *StandardObjectNameHistory* or *CustomObjectName__History*. For example, *AccountHistory* represents the history of changes to the values of an Account record's fields. Similarly, *MyCustomObject__History* tracks field history for the *MyCustomObject__c* custom object.

-  **Note:** Since the Spring '15 release, increasing the entity field history retention period beyond the standard 18–24 months requires the purchase of the Field Audit Trail add-on. When the add-on subscription is enabled, field history data is retained until you manually delete it. If your org was created before June 1, 2011, Salesforce continues to retain all field history. If your org was created on or after June 1, 2011 and you decide not to purchase the add-on, Salesforce retains your field history for the standard 18–24 months.

Considerations

Consider the following when working with field history tracking.

General Considerations

- Salesforce starts tracking field history from the date and time that you enable it on a field. Changes made before this date and time aren't included and didn't create an entry in the History related list.
- Use Data Loader or the `queryAll()` API to retrieve field history that's 18–24 months old.

- Changes to fields with more than 255 characters are tracked as edited, and their old and new values aren't recorded.
- Changes to time fields aren't tracked in the field history related list.
- The Field History Tracking timestamp is precise to a second in time. In other words, if two users update the same tracked field on the same record in the same second, both updates have the same timestamp. Salesforce can't guarantee the commit order of these changes to the database. As a result, the display values can look out of order.
- You can't create a record type on a standard or custom object and enable field history tracking on the record type in the same Metadata API deployment. Instead, create the record type in one deployment and enable history tracking on it in a separate deployment.
- Salesforce doesn't enable the recently viewed or referenced functionality in *StandardObjectNameHistory* or *CustomObjectName__History* objects. As a result, you can't use the FOR VIEW or FOR REFERENCE clauses in SOQL queries on these history objects. For example, the following SOQL query isn't valid:

```
SELECT AccountId, Field FROM AccountHistory LIMIT 1 FOR VIEW
```

Interactions with Other Salesforce Features

- In Lightning, you can see gaps in numerical order in the Created Date and ID fields. All tracked changes are still committed and recorded to your audit log. However, the exact time that those changes occur in the database can vary widely and aren't guaranteed to occur within the same millisecond. For example, there can be triggers or updates on a field that increase the commit time, and you can see a gap in time. During that time period, IDs are created in increasing numerical order but can also have gaps for the same reason.
- If Process Builder, an Apex trigger, or a Flow causes a change on an object the current user doesn't have permission to edit, that change isn't tracked. Field history honors the permissions of the current user and doesn't record changes that occur in system context.
- Salesforce attempts to track all changes to a history-tracked field, even if a particular change is never stored in the database. For example, let's say an admin defines an Apex before trigger on an object that changes a Postal Code field value of *12345* to *94619*. A user adds a record to the object and sets the Postal Code field to *12345*. Because of the Apex trigger, the actual Postal Code value stored in the database is *94619*. Although only one value was eventually stored in the database, the tracked history of the Zip Code field has two new entries:
 - No value --> *12345* (the change made by the user when they inserted the new record)
 - *12345* --> *94619* (the change made by the Apex trigger)

Event and Task History Considerations

- It can take up to a few minutes for changes to appear in history.
- You can track up to six fields on events or tasks.
- After an activity is deleted, the history for the activities can be visible via API queries for up to a few days. The history remains available because it's deleted asynchronously from the activity.
- Not all changes to recurring and child events are tracked.
- You can't delete specific field history records.
- Bulk processes such as Bulk API transactions or event syncing can be delayed when field history tracking is enabled. If processes are delayed, consider turning off activity field history tracking.
- The parent record of an activity is locked when the activity history updates. For example, if an activity is linked to thousands of accounts, each account is locked while the history updates. As a best practice, avoid [data skew](#). If processes fail because of parent-child row locking, consider turning off activity field history tracking.
- Field value changes caused by process builder, Apex triggers, or flows are tracked in an activity's history. Users see the change only if their field-level security settings permit them to. In other objects, field changes from processes, triggers, and flows are tracked only if the current user has permission to edit the modified fields.

- If a previously encrypted field used for tracking is unencrypted, the values tracked while the field was encrypted don't appear. After the field is unencrypted, the values are tracked in history.
- Activity history is available in APIs only for admins with permission to modify all data.
- For activities, field history is shown in a Lightning component that looks like a related list. Instead of managing the history on the page layout, you place the Activity Record History component on Lightning pages for event and task records. You can add the Activity Record History component to custom event and task pages or remove it from the default pages. The history list stays empty until you turn on field history tracking in the Object Manager.
- Fields displaying decimal values, such as currency and percent field types, aren't supported.
- The history list isn't available in Salesforce Classic or in the mobile app.

Contact History Considerations

- When a lead is converted to a new or an existing contact, the `contactCreatedFromLead` or `contactUpdatedByLead` field appears in the History related list for the contact. The presence of these fields in the contact history indicates that the contact was created or updated from a lead. The field value is always null.

Translation and Locale Considerations

- Tracked field values aren't automatically translated; they display in the language in which they were made. For example, if a field is changed from *Green* to *Verde*, *Verde* is displayed no matter what a user's language is, unless the field value has been translated into other languages via the Translation Workbench. This behavior also applies to record types and picklist values.
- Changes to custom field labels that have been translated via the Translation Workbench are shown in the locale of the user viewing the History related list. For example, if a custom field label is *Red* and translated into Spanish as *Rojo*, then a user with a Spanish locale sees the custom field label as *Rojo*. Otherwise, the user sees the custom field label as *Red*.
- Changes to date fields, number fields, and standard fields are shown in the locale of the user viewing the History related list. For example, a date change to *August 5, 2012* shows as *8/5/2012* for a user with the English (United States) locale, and as *5/8/2012* for a user with the English (United Kingdom) locale.

[Track Field History for Standard Objects](#)

You can enable field history tracking for standard objects in the object's management settings.

[Track Field History for Custom Objects](#)

You can enable field history tracking for custom objects in the object's management settings.

[Disable Field History Tracking](#)

You can turn off field history tracking from the object's management settings.

[Field Audit Trail](#)

With Field Audit Trail, you can define a policy to retain archived field history data. This feature helps you comply with industry regulations related to audit capability and data retention.

SEE ALSO:

[Track Field History for Standard Objects](#)

[Track Field History for Custom Objects](#)

[Field Audit Trail](#)

[Disable Field History Tracking](#)

[Salesforce Help: Export Data with Data Loader](#)

Track Field History for Standard Objects

You can enable field history tracking for standard objects in the object's management settings.

If you use both business accounts and person accounts, keep in mind that:

- Field history tracking for accounts applies to both business and person accounts, so the 20-field maximum includes both types of accounts.
- Changes made directly to a person contact record aren't tracked by field history.

To set up field history tracking:

1. From the management settings for the object whose field history you want to track, go to the fields area.

2. Click **Set History Tracking**.



Tip: When you enable tracking for an object, customize your page layouts to include the object's history related list.

3. For accounts, contacts, leads, and opportunities, select the `Enable Account History`, `Enable Contact History`, `Enable Lead History`, or `Enable Opportunity History` checkbox.

4. Choose the fields you want tracked.

You can select a combination of up to 20 standard and custom fields per object. For accounts, this limit includes fields for both business accounts and person accounts..

Certain changes, such as case escalations, are always tracked.

You can't track the following fields:

- Formula, roll-up summary, or auto-number fields
- `Created By` and `Last Modified By`
- Fields that have the `AI Prediction` checkbox selected
- `Expected Revenue` field on opportunities
- `Master Solution Title` or the `Master Solution Details` fields on solutions; these fields display only for translated solutions in organizations with multilingual solutions enabled.

5. Click **Save**.

Salesforce tracks history from this date and time forward. Changes made prior to this date and time are not included.

SEE ALSO:

[Field History Tracking](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)), Lightning Experience, and the Salesforce app

Available in: **Contact Manager, Essentials, Group, Professional, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

Standard Objects are not available in **Database.com**

USER PERMISSIONS

To set up which fields are tracked:

- Customize Application

Track Field History for Custom Objects

You can enable field history tracking for custom objects in the object's management settings.

1. From Setup, enter *Object Manager* in the Quick Find box, then select **Object Manager**.
2. Click the custom object, and click **Edit**.
3. Under Optional Features, select the `Track Field History` checkbox.



Tip: When you enable tracking for an object, customize your page layouts to include the object's history related list.

4. Save your changes.
5. Click `Set History Tracking` in the Custom Fields & Relationships section.
This section lets you set a custom object's history for both standard and custom fields.

6. Choose the fields you want tracked.

You can select up to 20 standard and custom fields per object. You can't track:

- Formula, roll-up summary, or auto-number fields
- `Created By` and `Last Modified By`
- Fields that have the `AI Prediction` checkbox selected

7. Click **Save**.

Salesforce tracks history from this date and time forward. Changes made prior to this date and time are not included.

Field History Tracking is supported on custom objects in managed packages. However, if the package developer updates the packaged field history settings, those settings aren't updated during package upgrades.

SEE ALSO:

[Field History Tracking](#)

[Find Object Management Settings](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)), Lightning Experience, and the Salesforce app

Available in: **Contact Manager, Essentials, Group, Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

Standard Objects aren't available in **Database.com**

USER PERMISSIONS

To set up which fields are tracked:

- `Customize Application`

Disable Field History Tracking

You can turn off field history tracking from the object's management settings.

 **Note:** If Apex references one of an object's fields, you can't disable field history tracking for that object.

1. From the management settings for the object whose field history you want to stop tracking, go to Fields.
2. Click `Set History Tracking`.
3. Deselect the enable history for the object you're working with—for example, **Enable Account History**, **Enable Contact History**, **Enable Lead History**, or **Enable Opportunity History**.

The History related list is automatically removed from the associated object's page layouts.

If you disable field history tracking on a standard object, you can still report on its history data up to the date and time that you disabled tracking. If you disable field history tracking on a custom object, you can't report on its field history.

4. Save your changes.

SEE ALSO:

[Field History Tracking](#)

Field Audit Trail

With Field Audit Trail, you can define a policy to retain archived field history data. This feature helps you comply with industry regulations related to audit capability and data retention.

 **Note:** Async SOQL is scheduled for retirement in all Salesforce orgs as of Summer '23.

Use Salesforce Metadata API to define a field history retention policy for those fields that have history tracking enabled. Then use REST API, SOAP API, and Tooling API to work with your archived data. For information about enabling Field Audit Trail, contact your Salesforce representative.

Field history is copied from the History related list into the `FieldHistoryArchive` big object. You define one `HistoryRetentionPolicy` for your related history lists, such as Account History, to specify Field Audit Trail retention policies for the objects that you want to archive. Then use Metadata API to deploy your policy. You can update the retention policy on an object as often as needed. With Field Audit Trail, you can track up to 60 fields per object. Without it, you can track only 20 fields per object. With Field Audit Trail, archived field history data is stored until you manually delete it. You can manually delete data that falls outside of your policy window.

 **Important:** Field history tracking data and Field Audit Trail data don't count against your data storage limits.

You can set field history retention policies on these objects.

- Accounts, including Person Accounts
- Assets
- Authorization Form Consent
- Campaigns

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)), Lightning Experience, and the Salesforce app

Available in: **Contact Manager, Essentials, Group, Professional, Enterprise, Performance, Unlimited, Developer**, and **Database.com** Editions

Standard Objects aren't available in **Database.com**

USER PERMISSIONS

To set up which fields are tracked:

- Customize Application

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)), Lightning Experience, and the Salesforce mobile app

Available in: **Enterprise, Performance**, and **Unlimited** Editions

USER PERMISSIONS

To specify a field history retention policy:

- Retain Field History

- Cases
- Communication Subscription Consent
- Contacts
- Contact Point Consent
- Contact Point Type Consent
- Contracts
- Contract Line Items
- Crisis
- Employee
- Employee Crisis Assessment
- Entitlements
- Individuals
- Internal Organization Unit
- Leads
- Opportunities
- Orders
- Order Products
- Party Consent
- Price Books
- Price Book Entries
- Products
- Service Appointments
- Service Contracts
- Solutions
- Work Orders
- Work Order Line Items
- Custom objects with field history tracking enabled

 **Note:** When Field Audit Trail is enabled, `HistoryRetentionPolicy` is automatically set on the supported objects. By default, data is archived after 18 months in production, after one month in sandboxes, and all archived data is stored until you manually delete it. The default retention policy isn't included when retrieving the object's definition through Metadata API. Only custom retention policies are retrieved along with the object definition.

You can include field history retention policies in managed and unmanaged packages.

These fields can't be tracked.

- Formula, roll-up summary, or auto-number fields
- Created By and Last Modified By
- Expected Revenue field on opportunities
- Master Solution Title or the Master Solution Details fields on solutions
- Long text fields
- Multi-select fields

After you define and deploy a Field Audit Trail policy, production data is migrated from related history lists such as Account History into the `FieldHistoryArchive` big object. The first copy writes the field history that's defined by your policy to archive storage and sometimes takes a long time. Subsequent copies transfer only the changes since the last copy and are faster. A bounded set of SOQL is available to query your archived data. If you delete a record in your production data, the delete cascades to the associated history tracking records, but the history copied into the `FieldHistoryArchive` big object isn't deleted. To delete data in `FieldHistoryArchive`, see [Delete Field History and Field Audit Trail Data](#).

Use Async SOQL to build aggregate reports from a custom object based on the volume of the data in the `FieldHistoryArchive` big object.

 **Important:** If you enable Platform Encryption in your org and use Field Audit Trail to track encrypted fields, there are limitations on using Async SOQL. Using Async SOQL to query the `NewValue` or `OldValue` fields of the `FieldHistoryArchive` big object isn't supported. Use SOQL to query both encrypted and unencrypted `NewValue` and `OldValue` fields of `FieldHistoryArchive`.

 **Tip:** Previously archived data remains unencrypted if you turn on Platform Encryption later. For example, your organization uses Field Audit Trail to define a data history retention policy for an account field, such as the phone number field. After enabling Platform Encryption, you turn on encryption for that field, and phone number data in the account is encrypted. New phone number records and previous updates stored in the Account History related list are encrypted. But phone number history data already archived in the `FieldHistoryArchive` object remains stored without encryption. To encrypt previously archived data, contact Salesforce to encrypt and rearchive the stored field history data, then delete the unencrypted archive.

Examples

Here are some examples of field history workflows.

SEE ALSO:

[Learning Map: Shield Learning Map](#)

[SOAP API Developer Guide: FieldHistoryArchive](#)

[Metadata API Developer Guide: HistoryRetentionPolicy](#)

[ISVforce Guide: Use Managed Packages to Develop Your AppExchange Solution](#)

[Lightning Platform SOQL and SOSL Reference: SOQL with Archived Data](#)

[Big Objects Implementation Guide: Async SOQL](#)

Examples

Here are some examples of field history workflows.

Set Data Retention Policy for Field History

This example demonstrates how to set a field history data retention policy using Metadata API. By default, field history data is not automatically deleted. Edit the metadata only if you want to override the default policy values of 18 months of production storage. Setting a data retention policy involves creating a metadata package and deploying it. The package consists of a `.zip` file and a project manifest that lists the objects and the API version to use. The `.zip` file contains an `objects` folder with the XML that defines each object's retention policy.

 **Note:** The first copy writes the entire field history that's defined by your policy to archive storage and takes a long time. Subsequent copies transfer only the changes since the last copy, and are faster.

Define a field history data retention policy for each object. The policy specifies the number of months that you want to maintain field history in Salesforce. The following sample file defines a policy of archiving the object after six months.

```
<?xml version="1.0" encoding="UTF-8"?>
<CustomObject xmlns="http://soap.sforce.com/2006/04/metadata">
  <historyRetentionPolicy>
    <archiveAfterMonths>6</archiveAfterMonths>
    <archiveRetentionYears>5</archiveRetentionYears>
    <description>My field history retention</description>
  </historyRetentionPolicy>
  ...
</CustomObject>
```

The file name determines the object to which the policy is applied. For example, to apply the preceding policy to the Account object, save the file as `Account.object`. For existing custom objects, the file is also named after the custom object. For example: `myObject__c.object`.

Create the project manifest, which is an XML file that's called `package.xml`. The following sample file lists several objects for which data retention policy is to be applied. With this manifest file, you expect the objects folder to contain five files: `Account.object`, `Case.object`, and so on.

```
<?xml version="1.0" encoding="UTF-8"?>
<Package xmlns="http://soap.sforce.com/2006/04/metadata">
  <types>
    <members>Account</members>
    <members>Case</members>
    <members>Contact</members>
    <members>Lead</members>
    <members>Opportunity</members>
    <name>CustomObject</name>
  </types>
  <version>45.0</version>
</Package>
```

Create the `.zip` file and use the `deploy()` function to deploy your changes to your production environment. For more information, see the [Metadata API Guide](#).

 **Note:** This feature doesn't support deployment from sandbox to production environments.

That's it! Your field history retention policy goes into effect according to the time periods that you set.

Create a Custom Object and Set Field History Retention Policy at the Same Time

You can use Metadata API to create a custom object and set retention policy at the same time. Specify the minimum required fields when creating a custom object. This sample XML creates an object and sets field history retention policy.

```
<?xml version="1.0" encoding="UTF-8"?>
<CustomObject xmlns="http://soap.sforce.com/2006/04/metadata">
  <deploymentStatus>Deployed</deploymentStatus>
  <enableHistory>true</enableHistory>
  <description>just a test object with one field for eclipse ide testing</description>
  <historyRetentionPolicy>
    <archiveAfterMonths>3</archiveAfterMonths>
    <archiveRetentionYears>10</archiveRetentionYears>
    <gracePeriodDays>1</gracePeriodDays>
```

```

    <description>Transaction Line History</description>
  </historyRetentionPolicy>
  <fields>
    <fullName>Comments__c</fullName>
    <description>add your comments about this object here</description>
    <inlineHelpText>This field contains comments made about this object</inlineHelpText>

    <label>Comments</label>
    <length>32000</length>
    <trackHistory>true</trackHistory>
    <type>LongTextArea</type>
    <visibleLines>30</visibleLines>
  </fields>
  <label>MyFirstObject</label>
  <nameField>
    <label>MyFirstObject Name</label>
    <type>Text</type>
  </nameField>
  <pluralLabel>MyFirstObjects</pluralLabel>
  <sharingModel>ReadWrite</sharingModel>
</CustomObject>

```

Set `trackHistory` to `true` on the fields that you want to track and `false` on the other fields.

Update Data Retention Policy for Field History

If a field history data retention policy is already defined on an object, you can update the policy by specifying a new value of `HistoryRetentionPolicy` in the metadata for that object. When you deploy the metadata changes, the new policy overwrites the previous one.



Note: To check the current data retention policy for any object, retrieve its metadata using Metadata API and look up the value of `HistoryRetentionPolicy`.

Query Archived Data

You can retrieve archived data by making SOQL queries on the `FieldHistoryArchive` object. You can filter on the `FieldHistoryType`, `ParentId`, and `CreatedDate` fields, as long as you specify them in that order. For example:

```

SELECT ParentId, FieldHistoryType, Field, Id, NewValue, OldValue FROM FieldHistoryArchive
WHERE FieldHistoryType = 'Account' AND ParentId='001D000000INjVe'

```

Monitor Debug Logs

Set trace flags to trigger logging for users, Apex classes, and Apex triggers in the Developer Console or in Setup. Monitor the resulting logs to diagnose problems in your org.

You can retain and manage debug logs for specific users, including yourself, and for classes and triggers. Setting class and trigger trace flags doesn't cause logs to be generated or saved. Class and trigger trace flags override other logging levels, including logging levels set by user trace flags, but they don't cause logging to occur. If logging is enabled when classes or triggers execute, logs are generated at the time of execution.

Set Up Debug Logging

To activate debug logging for users, Apex classes, and Apex triggers, configure trace flags and debug levels in the Developer Console or in Setup. Each trace flag includes a debug level, start time, end time, and log type. The trace flag's log type specifies the entity you're tracing.

View Debug Logs

The debug log contains information about each transaction, such as whether it was successful and how long it took. Depending on the filters set by your trace flags, the log can contain varying levels of detail about the transaction.

Set Up Debug Logging

To activate debug logging for users, Apex classes, and Apex triggers, configure trace flags and debug levels in the Developer Console or in Setup. Each trace flag includes a debug level, start time, end time, and log type. The trace flag's log type specifies the entity you're tracing.

You can retain and manage debug logs for specific users, including yourself, and for classes and triggers. Setting class and trigger trace flags doesn't cause logs to be generated or saved. Class and trigger trace flags override other logging levels, including logging levels set by user trace flags, but they don't cause logging to occur. If logging is enabled when classes or triggers execute, logs are generated at the time of execution.

Debug Log Limits

Debug logs have the following limits.

- Each debug log must be 20 MB or smaller. Debug logs that are larger than 20 MB are reduced in size by removing older log lines, such as log lines for earlier `System.debug` statements. The log lines can be removed from any location, not just the start of the debug log.
- System debug logs are retained for 24 hours. Monitoring debug logs are retained for seven days.
- If you generate more than 1,000 MB of debug logs in a 15-minute window, your trace flags are disabled. We send an email to the users who last modified the trace flags, informing them that they can re-enable the trace flag in 15 minutes.



Warning: If the debug log trace flag is enabled on a frequently accessed Apex class or for a user executing requests often, the request can result in failure, regardless of the time window and the size of the debug logs.

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#))

Available in **Enterprise, Developer, Performance, Unlimited,** and **Database.com** Editions

The Salesforce user interface and Email Services are not available in **Database.com**.

USER PERMISSIONS

To view, retain, and delete debug logs:

- View All Data

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To view, retain, and delete debug logs:

- View All Data

- When your org accumulates more than 1,000 MB of debug logs, we prevent users in the org from adding or editing trace flags. To add or edit trace flags so that you can generate more logs after you reach the limit, delete some debug logs.

Configure Trace Flags in the Developer Console

To configure trace flags and debug levels from the Developer Console, click **Debug > Change Log Levels**. Then complete these actions.

- To create a trace flag, click **Add**.
- To edit an existing trace flag's duration, double-click its start or end time.
- To change a trace flag's debug level, click **Add/Change** in the Debug Level Action column. You can then edit your existing debug levels, create or delete a debug level, and assign a debug level to your trace flag. Deleting a debug level deletes all trace flags that use it.

Create Trace Flags in Setup

1. From Setup, enter *Debug Logs* in the Quick Find box, then click **Debug Logs**.
2. Click **New**.
3. Select the entity to trace, the time period during which you want to collect logs, and a debug level. A debug level is a set of log levels for debug log categories: Database, Workflow, Validation, and so on. You can reuse debug levels across your trace flags.

New Trace Flag [Help for this Page](#)

To specify the type of information that is included in debug logs, add trace flags and debug levels. Each trace flag includes a debug level, a start time, an end time, and a log type.

Trace flags set logging levels (such as for Database, Workflow, and Validation) for a user, Apex class, or Apex trigger for up to 24 hours.

- Select **Automated Process** from the drop-down to set a trace flag on the automated process user. The automated process user runs background jobs, such as emailing Chatter invitations.
- Select **User** from the drop-down to specify a user whose debug logs you would like to monitor and retain.
- Select **Apex Class** or **Apex Trigger** from the drop-down to specify the log levels that take precedence while executing a specific Apex class or trigger. Setting class and trigger trace flags doesn't cause logs to be generated or saved. Class and trigger trace flags override other logging levels, including logging levels set by user trace flags, but they don't cause logging to occur. If logging is enabled when classes or triggers execute, logs are generated at the time of execution.

[Configure your Debug Levels.](#)

Traced Entity Type	Apex Class 
Traced Entity Name	SampleClass  
Start Date	8/11/2017 11:20 AM [8/11/2017 11:20 AM]
Expiration Date	8/11/2017 11:50 AM [8/11/2017 11:20 AM]
Debug Level 	ApexCodeFinest  <input type="button" value="New Debug Level"/>

View, Edit, or Delete Trace Flags in Setup

To manage trace flags from Setup, complete these actions.

1. Navigate to the appropriate Setup page.
 - For user-based trace flags, enter *Debug Logs* in the Quick Find box, then click **Debug Logs**.
 - For class-based trace flags, enter *Apex Classes* in the Quick Find box, click **Apex Classes**, click the name of a class, then click **Trace Flags**.
 - For trigger-based trace flags, enter *Apex Triggers* in the Quick Find box, click **Apex Triggers**, click the name of a trigger, then click **Trace Flags**.
2. From the Setup page, click an option in the Action column.
 - To delete a trace flag, click **Delete**.
 - To modify a trace flag, click **Edit**.
 - To modify a trace flag's debug level, click **Filters**.

- To create a debug level, click **Edit**, and then click **New Debug Level**.

Configure Debug Levels in Setup

To manage your debug levels from Setup, enter *Debug Levels* in the Quick Find box, then click **Debug Levels**. To edit or delete a debug level, click an option in the Action column. To create a debug level, click **New**.

Action	Name	Workflow	Validation	Callout	Apex Code	Apex Profiling	Visualforce	System	Database
Edit Del	ApexCodeFinest	None	None	None	Finest	None	None	None	None
Edit Del	MostlyInfoApexSystemDebug	Info	Info	Info	Debug	Info	Info	Debug	Info

Collect Debug Logs for Guest Users

Your public users generate a large volume of events, which can quickly fill up your debug logs. When collecting debug logs for guest users, keep in mind that all your public site visitors share one guest user license. One Salesforce user represents all your site's public users.

To enable logging for your public users:

- Find the name of your site's guest user.
 - From Setup, enter *Sites* in the Quick Find box, then select **Sites**.
 - Select your site from the Site Label column.
 - Select **Public Access Settings > View Users**.
- Set a user-based trace flag on the guest user.
 - From Setup, enter *Debug Logs* in the Quick Find box, then click **Debug Logs**.
 - Click **New**.
 - Set the traced entity type to **User**.
 - Open the lookup for the Traced Entity Name field, and then find and select your guest user.
 - Assign a debug level to your trace flag.
 - Click **Save**.



Tip: Debug logs are for live troubleshooting. To record all site traffic, use event monitoring. For details, see [EventLogFile](#) in the *Salesforce Object Reference*.

SEE ALSO:

[Monitor Debug Logs](#)

[Delete Debug Logs](#)

View Debug Logs

The debug log contains information about each transaction, such as whether it was successful and how long it took. Depending on the filters set by your trace flags, the log can contain varying levels of detail about the transaction.

To view a debug log, from Setup, enter *Debug Logs* in the *Quick Find* box, then select **Debug Logs**. Then click **View** next to the debug log that you want to examine. Click **Download** to download the log as an XML file.

Debug Log Limits

Debug logs have the following limits.

- Each debug log must be 20 MB or smaller. Debug logs that are larger than 20 MB are reduced in size by removing older log lines, such as log lines for earlier `System.debug` statements. The log lines can be removed from any location, not just the start of the debug log.
- System debug logs are retained for 24 hours. Monitoring debug logs are retained for seven days.
- If you generate more than 1,000 MB of debug logs in a 15-minute window, your trace flags are disabled. We send an email to the users who last modified the trace flags, informing them that they can re-enable the trace flag in 15 minutes.



Warning: If the debug log trace flag is enabled on a frequently accessed Apex class or for a user executing requests often, the request can result in failure, regardless of the time window and the size of the debug logs.

- When your org accumulates more than 1,000 MB of debug logs, we prevent users in the org from adding or editing trace flags. To add or edit trace flags so that you can generate more logs after you reach the limit, delete some debug logs.

SEE ALSO:

[Monitor Debug Logs](#)

[Delete Debug Logs](#)

EDITIONS

Available in: Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To view, retain, and delete debug logs:

- [View All Data](#)

Monitoring Scheduled Jobs

The All Scheduled Jobs page lists all reporting snapshots, scheduled Apex jobs, and dashboards scheduled to refresh.

To view this page, from Setup, enter *Scheduled Jobs* in the Quick Find box, then select **Scheduled Jobs**. Depending on your permissions, you can perform some or all of the following actions.

- Click **Del** to permanently delete all instances of a scheduled job.
- View the details of a scheduled job, such as the:
 - Name of the scheduled job
 - Name of the user who submitted the scheduled job
 - Date and time at which the scheduled job was originally submitted
 - Date and time at which the scheduled job started
 - Next date and time at which the scheduled job will run
 - Type of scheduled job

Monitor Background Jobs

You can monitor background jobs in your organization, such as when parallel sharing recalculation is running.

Parallel sharing recalculation helps larger organizations to speed up sharing recalculation of each object.

 **Note:** You can only monitor background jobs on this page. Contact Salesforce to abort a background job.

1. From Setup, in the Quick Find box, enter *Background Jobs*, and then select **Background Jobs**.
2. Review details of background jobs, which include a percentage estimate of the recalculation progress.
 - The **Job Type** column shows the background job that's running, such as *Organization-Wide Default Update*.
 - The **Job Sub Type** column shows the affected object, such as *Account* or *Opportunity*, or the phase of the recalculation process, such as *Person Account Access*, *Associated Portal Account Access*, or *Parent Account Access*.

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

Reporting Snapshots and Dashboards are not available in **Database.com**

USER PERMISSIONS

To monitor scheduled jobs:

- View Setup and Configuration

EDITIONS

Available in: both Salesforce Classic ([not available in all orgs](#)) and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To monitor background jobs:

- View Setup and Configuration

When the Job's **Status** is listed as `Completed`, sometimes additional operations must still finish before the changes are reflected in your organization. Depending on the operation, this process can take significant time.

SEE ALSO:

[Recalculate Sharing Rules Manually](#)

[Automatic Recalculation of Org-Wide Defaults and Sharing Rules](#)

Manage Bulk Data Load Jobs

You can create update, or delete a large volume of records with the Bulk API, which is optimized for processing large sets of data. It makes it simple to load, update, or delete data from a few thousand to millions of records.

[Monitor Bulk Data Load Jobs](#)

Process a set of records by creating a job that contains data that will be processed asynchronously. The job specifies which object is being processed and what type of operation is being used.

[View Bulk Data Load Job Details](#)

When you create update, or delete a large volume of records with the Bulk API or Bulk API 2.0, each job has a Job Detail page where you can monitor the progress of the job.

SEE ALSO:

[Introduction to Bulk API 2.0](#)

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

USER PERMISSIONS

To monitor bulk data load jobs:

- Manage Data Integrations, API Enabled, View Setup and Configuration

Monitor Bulk Data Load Jobs

Process a set of records by creating a job that contains data that will be processed asynchronously. The job specifies which object is being processed and what type of operation is being used.

To track the status of bulk data load jobs that are in progress or recently completed, enter *Bulk Data Load Jobs* in the **Quick Find** box, then select **Bulk Data Load Jobs**. This page allows you to monitor the progress of current jobs and the results of recent jobs.

The In Progress Jobs list contains the following columns, shown in alphabetical order:

Column	Description
Job ID	The unique, 15-character ID for this job.
Job Type	The API type used for the job. Valid values are 'Bulk V1', 'Bulk V2', and 'Bulk V2 Query'. Bulk V2 and Bulk V2 Query jobs use the newer Bulk API 2.0 for creating and processing job data. Bulk API 2.0 simplifies the job process by automatically creating batches.
Object	The object type for the data being processed. All data in a job must be of a single object type.
Operation	The processing operation for all the batches in the job. Possible values are: <ul style="list-style-type: none"> Delete Insert Query QueryAll Upsert Update HardDelete
Progress	The percentage of batches processed relative to the total number of batches submitted. Progress is not shown when the job is open because the total number of batches in the job is not known until the job is closed. Progress may not accurately reflect the number of records processed. Batches may not all contain the same number of records and they may be processed at different speeds.
Records Processed	The number of records already processed. This number increases as more batches are processed.
Start Time	The date and time when the job was submitted.
Status	The current state of processing for the job. The valid values are: <ul style="list-style-type: none"> Open: The job has been created, and data can be added to the job. Closed: No new data can be added to this job. Data associated with the job may be processed after a job is closed. You cannot edit or save a closed job. Aborted: The job has been aborted. Failed: The job has failed. Data that was successfully processed in the job cannot be rolled back.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To monitor bulk data load jobs:

- Manage Data Integrations, API Enabled, View Setup and Configuration

Column	Description
	<ul style="list-style-type: none"> • Job Complete: The job was processed by Salesforce. For Bulk API 2.0 jobs only. • Upload Complete: No new data can be added to this job. You can't edit or save a closed job. For Bulk API 2.0 jobs only.
Submitted By	The name of the user that submitted the job.

The Completed Jobs list contains the following columns, shown in alphabetical order. Completed jobs are removed from the list seven days after completion.

Column	Description
End Time	The date and time when the job completed.
Job ID	The unique, 15-character ID for this job.
Job Type	The API type used for the job. Valid values are 'Bulk V1', 'Bulk V2', and 'Bulk V2 Query'. Bulk V2 and Bulk V2 Query jobs use the newer Bulk API 2.0 for creating and processing job data. Bulk API 2.0 simplifies the job process by automatically creating batches.
Object	The object type for the data being processed. All data in a job must be of a single object type.
Operation	The processing operation for all the batches in the job. The valid values are: <ul style="list-style-type: none"> • Delete • Insert • Query • QueryAll • Upsert • Update • HardDelete
Records Processed	The number of records already processed. This number increases as more batches are processed.
Start Time	The date and time when the job was submitted.
Status	The current state of processing for the job. The valid values are: <ul style="list-style-type: none"> • Open: The job has been created, and data can be added to the job. • Closed: No new data can be added to this job. Data associated with the job may be processed after a job is closed. You cannot edit or save a closed job. • Aborted: The job has been aborted. • Failed: The job has failed. Data that was successfully processed in the job cannot be rolled back. • Job Complete: The job was processed by Salesforce. For Bulk API 2.0 jobs only. • Upload Complete: No new data can be added to this job. You can't edit or save a closed job. For Bulk API 2.0 jobs only.
Submitted By	The name of the user that submitted the job.

Column	Description
Time to Complete	The total time to complete the job.

SEE ALSO:

[View Bulk Data Load Job Details](#)

[Introduction to Bulk API 2.0](#)

View Bulk Data Load Job Details

When you create update, or delete a large volume of records with the Bulk API or Bulk API 2.0, each job has a Job Detail page where you can monitor the progress of the job.

1. From Setup, enter *Bulk Data Load Jobs* in the Quick Find box, then select **Bulk Data Load Jobs**.
2. Click a Job ID link for a job.

The job detail page contains the following fields, shown in alphabetical order:

Field	Description
Apex Processing Time (ms)	The number of milliseconds taken to process triggers and other processes related to the job data. This is the sum of the equivalent times in all batches in the job. This doesn't include the time used for processing asynchronous and batch Apex operations. If there are no triggers, the value is 0.
API Active Processing Time (ms)	The number of milliseconds taken to actively process the job and includes the time tracked in the Apex Processing Time (ms) field, but doesn't include the time the job waited in the queue to be processed or the time required for serialization and deserialization. This is the sum of the equivalent times in all batches in the job.
API Version	The API version for the job.
Completed Batches	The number of batches that have been completed for this job.
Concurrency Mode	The concurrency mode for processing batches. The valid values are: <ul style="list-style-type: none"> • <code>parallel</code>: Batches are processed in parallel mode. This is the default value. • <code>serial</code>: Batches are processed in serial mode.
Content Type	The content type for the job. The valid values are: <ul style="list-style-type: none"> • <code>CSV</code>—data in CSV format (default and only supported content type for Bulk V2 type jobs) • <code>JSON</code>—data in JSON format • <code>XML</code>—data in XML format (default option for Bulk V1 type jobs) • <code>ZIP_CSV</code>—data in CSV format in a zip file containing binary attachments

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise, Performance, Unlimited, Developer,** and **Database.com** Editions

USER PERMISSIONS

To monitor bulk data load jobs:

- Manage Data Integrations, API Enabled, View Setup and Configuration

Field	Description
	<ul style="list-style-type: none"> • ZIP_JSON—data in JSON format in a zip file containing binary attachments • ZIP_XML—data in XML format in a zip file containing binary attachments
End Time	The date and time when the job completed.
External ID Field	The name of the external ID field for an <code>upsert()</code> .
Failed Batches	The number of batches that have failed for this job.
Job ID	The unique, 15-character ID for this job.
Job Type	The API type used for the job. Valid values are 'Bulk V1', 'Bulk V2', and 'Bulk V2 Query'. Bulk V2 and Bulk V2 Query jobs use the newer Bulk API 2.0 for creating and processing job data. Bulk API 2.0 simplifies the job process by automatically creating batches.
In Progress Batches	The number of batches that are in progress for this job.
Object	The object type for the data being processed. All data in a job must be of a single object type.
Operations	The processing operation for all the batches in the job. Possible values are: <ul style="list-style-type: none"> • Delete • Insert • Query • QueryAll • Upsert • Update • HardDelete
Progress	The percentage of batches processed relative to the total number of batches submitted. Progress isn't shown when the job is open because the total number of batches in the job isn't known until the job is closed. Progress may not accurately reflect the number of records processed. Batches may not all contain the same number of records and they might be processed at different speeds.
Queued Batches	The number of batches queued for this job.
Records Failed	The number of records that weren't processed successfully in this job.
Records Processed	The number of records processed at the time the request was sent. This number increases as more batches are processed.
Retries	The number of times that Salesforce attempted to save the results of an operation. The repeated attempts are due to a problem, such as a lock contention.
Start Time	The date and time when the job was submitted.

Field	Description
Status	The current state of processing for the job. The valid values are: <ul style="list-style-type: none"> • Open: The job has been created, and data can be added to the job. • Closed: No new data can be added to this job. Data associated with the job may be processed after a job is closed. You can't edit or save a closed job. • Aborted: The job has been aborted. • Failed: The job has failed. Data that was successfully processed in the job can't be rolled back. • Job Complete: The job was processed by Salesforce. For Bulk API 2.0 jobs only. • Upload Complete: No new data can be added to this job. You can't edit or save a closed job. For Bulk API 2.0 jobs only.
Submitted By	The name of the user that submitted the job.
Time to Complete	The total time to complete the job.
Total Processing Time (ms)	The number of milliseconds taken to process the job. This is the sum of the total processing times for all batches in the job.

The job detail page includes a related list of all the batches for the job. The related list provides **View Request** and **View Response** links for each batch. If the batch is a CSV file, the links return the request or response in CSV format. If the batch is an XML or JSON file, the links return the request or response in XML or JSON format, respectively. These links are available for batches created in API version 19.0 and later. For Bulk V2 type jobs, batch information is unavailable.

The batch related list contains the following fields, shown in alphabetical order:

Field	Description
Apex Processing Time (ms)	The number of milliseconds taken to process triggers and other processes related to the batch data. If there are no triggers, the value is 0. This doesn't include the time used for processing asynchronous and batch Apex operations.
API Active Processing Time (ms)	The number of milliseconds taken to actively process the batch, and includes Apex processing time. This doesn't include the time the batch waited in the queue to be processed or the time required for serialization and deserialization.
Batch ID	The ID of the batch. Can be globally unique, but doesn't have to be.
End Time	The date and time in the UTC time zone that processing ended. This is only valid when the state is Completed.
Records Failed	The number of records that weren't processed successfully in this batch.
Records Processed	The number of records processed in this batch at the time the request was sent. This number increases as more batches are processed.
Retry Count	The number of times that Salesforce attempted to save the results of an operation. The repeated attempts are due to a problem, such as lock contention or a batch taking too long to process.

Field	Description
Start Time	The date and time in the UTC time zone when the batch was created. This isn't the time processing began, but the time the batch was added to the job.
State Message	Contains the reasons for failure if the batch didn't complete successfully.
Status	The current state of processing for the batch: <ul style="list-style-type: none"> • Queued: Processing of the batch hasn't started yet. If the job associated with this batch is aborted, the batch isn't processed and its state is set to NotProcessed. • In Progress: The batch is being processed. If the job associated with the batch is aborted, the batch is still processed to completion. You must close the job associated with the batch so that the batch can finish processing. • Completed: The batch has been processed completely, and the result resource is available. The result resource indicates if some records have failed. A batch can be completed even if some or all the records have failed. If a subset of records failed, the successful records aren't rolled back. • Failed: The batch failed to process the full request due to an unexpected error, such as the request is compressed with an unsupported format, or an internal server error. • Not Processed: The batch failed to process the full request due to an unexpected error, such as the request is compressed with an unsupported format, or an internal server error.
Total Processing Time (ms)	The number of milliseconds taken to process the batch. This excludes the time the batch waited in the queue to be processed.
View Request	Click the link for a batch to see the request. Bulk V1 type jobs only.
View Result	Click the link for a batch to see the results. Bulk V1 type jobs only.

SEE ALSO:

[Monitor Bulk Data Load Jobs](#)

[Introduction to Bulk API 2.0](#)

Installed Packages

You can install packages into your Salesforce organization, and then configure and manage them.

To view the packages you've installed, from Setup, enter *Installed* in the Quick Find box, and then select **Installed Packages**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited,** and **Developer Editions**

Install a Package

Install a managed package in your Salesforce org to add new functionality to your org. Choose a custom installation to modify the default package settings, including limiting access to the package. Before you install a package, verify that the AppExchange listing is compatible with your Salesforce edition.

1. Determine your package access settings.

- Click **View Components**. You see an overlay with a list of components in the package. For managed packages, the screen also contains a list of connected apps (trusted applications that are granted access to a user's Salesforce data after the user and the application are verified). To confirm that the components and any connected apps shown are acceptable, review the list and then close the overlay.

 **Note:** Some package items, such as validation rules, record types, or custom settings don't appear in the Package Components list but are included in the package and installed with the other items. If there are no items in the Package Components list, it's likely that the package contains only minor changes.

- If the package contains a remote site setting, you must approve access to websites outside of Salesforce. The dialog box lists all the websites that the package communicates with. We recommend that a website uses SSL (secure sockets layer) for transmitting data. After you verify that the websites are safe, select **Yes, grant access to these third-party websites** and click **Continue**, or click **Cancel** to cancel the installation of the package.

 **Warning:** By installing remote site settings, you're allowing the package to transmit data to and from a third-party website. Before using the package, contact the publisher to understand what data is transmitted and how it's used. If you have an internal security contact, ask the contact to review the application so that you understand its impact before use.

- Click **API Access**. You see an overlay with a list of the API access settings that package components have been granted. Review the settings to verify they're acceptable, and then close the overlay to return to the installer screen.
- In Enterprise, Performance, Unlimited, and Developer Editions, choose one of the following security options.

 **Note:** This option is visible only in specific types of installations. For example, in Group and Professional Editions, or if the package doesn't contain a custom object, Salesforce skips this option, which gives all users full access.

Install for Admins Only

Specifies the following settings on the installing administrator's profile and any profile with the "Customize Application" permission.

- Object permissions—Read, Create, Edit, Delete, View All, and Modify All enabled
- Field-level security—set to visible and editable for all fields
- Apex classes—enabled
- Visualforce pages—enabled
- App settings—enabled
- Tab settings—determined by the package developer
- Page layout settings—determined by the package developer
- Record Type settings—determined by the package developer

After installation, if you have Enterprise, Performance, Unlimited, or Developer Edition, set the appropriate user and object permissions on custom profiles as needed.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To install packages:

- Download AppExchange Packages

Install for All Users

Specifies the following settings on all internal custom profiles.

- Object permissions— Read, Create, Edit, and Delete enabled
- Field-level security—set to visible and editable for all fields
- Apex classes—enabled
- Visualforce pages—enabled
- App settings—enabled
- Tab settings—determined by the package developer
- Page layout settings—determined by the package developer
- Record Type settings—copied from admin profile

 **Note:** The Customer Portal User, Customer Portal Manager, High Volume Customer Portal, Authenticated Website, Partner User, and standard profiles receive no access.

Install for Specific Profiles...

Lets you determine package access for all custom profiles in your org. You can set each profile to have full access or no access for the new package and all its components.

- Full Access—Specifies the following settings for each profile.
 - Object permissions Read, Create, Edit, and Delete enabled
 - Field-level security—set to visible and editable for all fields
 - Apex classes—enabled
 - Visualforce pages—enabled
 - App settings—enabled
 - Tab settings—enabled
 - Page layout settings—determined by the package developer
 - Record Type settings—determined by the package developer
- No Access—Page layout and Record Type settings are determined by the package developer. All other settings are hidden or disabled.

If the package developer has included settings for custom profiles, you can incorporate the settings of the publisher's custom profiles into your profiles without affecting your settings. Choose the name of the profile settings in the dropdown list next to the profile that you're applying them to. The current settings in that profile remain intact.

Alternatively, click **Set All** next to an access level to give this setting to all user profiles.

2. Click **Install**. You'll see a message that describes the progress and a confirmation message after the installation is complete.
 - During installation, Salesforce checks and verifies dependencies. An installer's organization must meet all dependency requirements listed on the Show Dependencies page or else the installation fails. For example, the installer's organization must have divisions enabled to install a package that references divisions.
 - When you install a component that contains Apex, all unit tests for your organization are run, including the unit tests contained in the new package. If a unit test relies on a component that is initially installed as inactive, such as a workflow rule, this unit test fails. You can select to install regardless of unit test failures.
 - If your installation fails, see [Why did my installation or upgrade fail?](#)

Pre-Installation Steps

1. In a browser, go to the installation URL provided by the package developer, or, if you're installing a package from AppExchange, click **Get It Now** from the application information page.
2. Enter your username and password for the Salesforce organization in which you want to install the package, and then click **Log In**.
3. Select **Install in Production** or **Install in Sandbox**.



Note: If you're installing into a sandbox, replace the `www.salesforce.com` portion of the package installation link with `test.salesforce.com`. The package is removed from your sandbox organization whenever you create a sandbox copy.

4. Accept the terms and conditions, then click **Confirm and Install**.
5. Enter org's login credentials. After you're directed to the appropriate org, continue with the package installation steps.
 - If the package is password-protected, enter the password you received from the publisher.
 - Optionally, if you're installing an unmanaged package, select **Rename Conflicting Components in Package**. When you select this option, Salesforce changes the name of a component in the package if its name conflicts with an existing component name.

Default Installation

Click **Install**. You'll see a message that describes the progress and a confirmation message after the installation is complete.

Custom Installation

To modify the default settings:

1. Determine your package access settings.
 - Click **View Components**. You see an overlay with a list of components in the package. For managed packages, the screen also contains a list of connected apps (trusted applications that are granted access to a user's Salesforce data after the user and the application are verified). To confirm that the components and any connected apps shown are acceptable, review the list and then close the overlay.
 -  **Note:** Some package items, such as validation rules, record types, or custom settings don't appear in the Package Components list but are included in the package and installed with the other items. If there are no items in the Package Components list, it's likely that the package contains only minor changes.
 - If the package contains a remote site setting, you must approve access to websites outside of Salesforce. The dialog box lists all the websites that the package communicates with. We recommend that a website uses SSL (secure sockets layer) for transmitting data. After you verify that the websites are safe, select **Yes, grant access to these third-party websites** and click **Continue**, or click **Cancel** to cancel the installation of the package.
 -  **Warning:** By installing remote site settings, you're allowing the package to transmit data to and from a third-party website. Before using the package, contact the publisher to understand what data is transmitted and how it's used. If you have an internal security contact, ask the contact to review the application so that you understand its impact before use.
 - Click **API Access**. You see an overlay with a list of the API access settings that package components have been granted. Review the settings to verify they're acceptable, and then close the overlay to return to the installer screen.
 - In Enterprise, Performance, Unlimited, and Developer Editions, choose one of the following security options.
 -  **Note:** This option is visible only in specific types of installations. For example, in Group and Professional Editions, or if the package doesn't contain a custom object, Salesforce skips this option, which gives all users full access.

Install for Admins Only

Specifies the following settings on the installing administrator's profile and any profile with the "Customize Application" permission.

- Object permissions—Read, Create, Edit, Delete, View All, and Modify All enabled
- Field-level security—set to visible and editable for all fields
- Apex classes—enabled
- Visualforce pages—enabled
- App settings—enabled
- Tab settings—determined by the package developer
- Page layout settings—determined by the package developer
- Record Type settings—determined by the package developer

After installation, if you have Enterprise, Performance, Unlimited, or Developer Edition, set the appropriate user and object permissions on custom profiles as needed.

Install for All Users

Specifies the following settings on all internal custom profiles.

- Object permissions— Read, Create, Edit, and Delete enabled
- Field-level security—set to visible and editable for all fields
- Apex classes—enabled
- Visualforce pages—enabled
- App settings—enabled
- Tab settings—determined by the package developer
- Page layout settings—determined by the package developer
- Record Type settings—copied from admin profile



Note: The Customer Portal User, Customer Portal Manager, High Volume Customer Portal, Authenticated Website, Partner User, and standard profiles receive no access.

Install for Specific Profiles...

Lets you determine package access for all custom profiles in your org. You can set each profile to have full access or no access for the new package and all its components.

- Full Access—Specifies the following settings for each profile.
 - Object permissions—Read, Create, Edit, and Delete enabled
 - Field-level security—set to visible and editable for all fields
 - Apex classes—enabled
 - Visualforce pages—enabled
 - App settings—enabled
 - Tab settings—enabled
 - Page layout settings—determined by the package developer
 - Record Type settings—determined by the package developer
- No Access—Page layout and Record Type settings are determined by the package developer. All other settings are hidden or disabled.

If the package developer has included settings for custom profiles, you can incorporate the settings of the publisher's custom profiles into your profiles without affecting your settings. Choose the name of the profile settings in the dropdown list next to the profile that you're applying them to. The current settings in that profile remain intact.

Alternatively, click **Set All** next to an access level to give this setting to all user profiles.

2. Click **Install**. You'll see a message that describes the progress and a confirmation message after the installation is complete.
 - During installation, Salesforce checks and verifies dependencies. An installer's organization must meet all dependency requirements listed on the Show Dependencies page or else the installation fails. For example, the installer's organization must have divisions enabled to install a package that references divisions.
 - When you install a component that contains Apex, all unit tests for your organization are run, including the unit tests contained in the new package. If a unit test relies on a component that is initially installed as inactive, such as a workflow rule, this unit test fails. You can select to install regardless of unit test failures.
 - If your installation fails, see [Why did my installation or upgrade fail?](#)

Post-Installation Steps

If the package includes post-installation instructions, they're displayed after the installation is completed. Review and follow the instructions provided. In addition, before you deploy the package to your users, make any necessary changes for your implementation. Depending on the contents of the package, some of the following customization steps are required.

- If the package includes permission sets, assign the included permission sets to your users who need them. In managed packages, you can't edit permission sets that are included in the package, but subsequent upgrades happen automatically. If you clone a permission set that comes with a managed package or create your own, you can edit the permission set, but subsequent upgrades won't affect it.
- If you're reinstalling a package and need to reimport the package data by using the export file that you received after uninstalling, see [Import Package Data](#).
- If you installed a managed package, click **Manage Licenses** to assign licenses to users.
 -  **Note:** You can't assign licenses in Lightning Experience. To assign a license, switch to Salesforce Classic.
- Configure components in the package as required. For more information, see [Configuring Installed Packages](#).

Configuring Installed Packages

Many have an `isDeployed` attribute that controls whether they're available for end users. After installation, all components are immediately available if they were available in the developer's organization. Before making the package available to your users, make any necessary changes for your implementation.

. Depending on the contents of the package, you might need to customize the following items:

Configure Option

If the publisher included a link to an external website with information about configuration, AppExchange Downloads page displays a **Configure** option next to the package in Setup when you click **Installed Packages**. Click **Configure** to view the publisher's suggested configurations.

Custom Fields and Custom Links

Add any necessary custom fields or links to the new custom objects.

Custom Object

Enable tracking on objects that aren't in this package, but that have fields that are tracked in Chatter. For example, if you want to track a custom field on Account, you must make sure the Account standard object is enabled for tracking.

Custom Report Types

If the `Report Type Name` of a custom report type matches one used within your organization, change the `Report Type Name` after you install the package to avoid any confusion between the two report types.

Dashboard Running User

The `Running User` for any dashboards are set to the user installing the package. You can edit the properties of the dashboard and change the `Running User` to a user that has the security settings you want applied to the dashboard.

Folders

When apps contain documents, email templates, reports, or dashboards, Salesforce creates new folders in the installer's organization using the publisher's folder names. Make sure these folder names are unique in your organization.

All users can see new folders. Configure folder settings before you deploy if you want them to have limited visibility.

Home Page Layouts

Custom home page layouts included in the package are not assigned to any users. To make them available to your users, assign them to the appropriate profiles.

List Views

List views included in apps are visible to all users. Change the visibility of these list views if necessary.

Page Layouts

All users are assigned the default page layout for any custom objects included in the package. Administrators of Enterprise, Unlimited, Performance, and Developer Edition organizations can configure the page layout for the appropriate users.

If a custom object in the package includes any relationships to standard objects, add them as related lists on the appropriate page layouts.

If the package includes any custom links, add them to the appropriate page layouts.

If your organization has advanced currency management enabled, currency roll-up summary fields are invalid if they are on accounts and summarizing opportunity values, or on opportunities and summarizing custom object values. Remove these fields from any page layouts.

Permission Sets

Assign permission sets included in a package to the users who need access to the package.

EDITIONS

Available in: Salesforce Classic (not available in all orgs)

Available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer Editions**

USER PERMISSIONS

To install packages:

- Download AppExchange Packages

To configure installed packages:

- Customize Application

You can't edit permission sets that are included in a managed package. If you clone a permission set that comes with the package or create your own, you can make changes to the permission set, but subsequent upgrades won't affect it.

Records Created During Post-Installation Scripts

To edit records created by a post-install script, reassign the owner of the records to someone in your org. By default, records created during a post-install script are assigned to the APP account owner alias and can't be shared or edited.

Translation Workbench

Translated values for installed package components are also installed for any language that the developer has included. Any package components the developer has customized within setup, such as a custom field or record type, display in the installer's setup pages in the developer's language (the language used when defining these components). Users in the installer's organization automatically see translated values if their personal language is included in the package. Additionally, installers can activate additional languages as long as the Translation Workbench is enabled.

Workflow Alerts

If the recipient of a workflow alert is a user, Salesforce replaces that user with the user installing the package. You can change the recipients of any installed workflow alerts.

Workflow Field Updates

If a field update is designed to change a record owner field to a specific user, Salesforce replaces that user with the user installing the package. You can change the field value of any installed field updates.

Workflow Outbound Messages

Salesforce replaces the user in the `User to send as` field of an outbound message with the user installing the package. You can change this value after installation.

Workflow Rules

Workflow rules are installed without any time-based triggers that the developer might have created. Set up time-based triggers as necessary.

Workflow Tasks

Salesforce replaces the user in the `Assigned To` field with the user installing the package. You can change this value after installation.

Make any more customizations that are necessary for your implementation.

 **Note:** Anything you add to a custom app after installation will be removed with the custom app if you ever uninstall it.

SEE ALSO:

[Installed Packages](#)

[Tradeoffs and Limitations of Shield Platform Encryption](#)

Uninstall a Managed Package

Uninstalling a managed package removes its components and data from the org. During the uninstall process, any customizations, including custom fields or links, that you've made to the package are removed.

If you choose to save a copy of the package data, we create an export file containing the package data, associated notes, and any attachments. When the uninstall is complete, we send an email containing a link to the export file to the user performing the uninstall. We delete export files two days after a completed package uninstall.

1. From Setup, enter *Installed Packages* in the Quick Find box, then select **Installed Packages**.
2. Click **Uninstall** next to the package that you want to remove.
3. Determine whether to save and export a copy of the package's data, and then select the corresponding radio button.
4. Select **Yes, I want to uninstall** and click **Uninstall**.
 - If you're uninstalling a package that includes a custom object, all components on that custom object are also deleted. Deleted items include custom fields, validation rules, custom buttons, and links, workflow rules, and approval processes.
 - You can't uninstall a package whenever a component not included in the uninstall references any component in the package. For example:
 - When an installed package includes any component on a standard object that another component references, Salesforce prevents you from uninstalling the package. An example is a package that includes a custom user field with a workflow rule that gets triggered when the value of that field is a specific value. Uninstalling the package would prevent your workflow from working.
 - When you've installed two unrelated packages that each include a custom object and one custom object component references a component in the other, you can't uninstall the package. An example is if you install an expense report app that includes a custom user field and create a validation rule on another installed custom object that references that custom user field. However, uninstalling the expense report app prevents the validation rule from working.
 - When an installed folder contains components you added after installation, Salesforce prevents you from uninstalling the package.
 - When an installed letterhead is used for an email template you added after installation, Salesforce prevents you from uninstalling the package.
 - When an installed package includes a custom field that's referenced by Einstein Prediction Builder or Case Classification, Salesforce prevents you from uninstalling the package. Before uninstalling the package, edit the prediction in Prediction Builder or Case Classification so that it no longer references the custom field.
 - You can't uninstall a package that removes all active business and person account record types. Activate at least one other business or person account record type, and try again.
 - You can't uninstall a package if a background job is updating a field added by the package, such as an update to a roll-up summary field. Wait until the background job finishes, and try again.

EDITIONS

Available in: both Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

USER PERMISSIONS

To uninstall packages:

- **Download AppExchange Packages**

Manage Installed Packages

Manage packages installed in your Salesforce org, including assigning licenses to users, uninstalling packages, and exporting package data.

 **Note:** Salesforce only lists license information for managed packages. For unmanaged packages, the license-related fields, such as **Allowed Licenses**, **Used Licenses**, and **Expiration Date**, displays the value "N/A."

Using this list, you can:

- Click **Uninstall** to remove the package and all its components from your Salesforce organization.
- Click **Manage Licenses** to assign available licenses to users in your organization.

If you purchased a site license or if the managed package is not licensed, Salesforce assigns licenses to all your users and you can't manage licenses. Your users can use the package as long as they have the appropriate permissions.

 **Note:** Certain managed packages created by Salesforce, require external access to data within your org. To grant access to allow an installed managed package to connect with external data, click **Enable for Platform Integrations**. Alternatively, to revoke access between an installed managed package and external data, click **Disable for Platform Integrations**. Enable this functionality, only upon request from a Salesforce-owned managed package.

- Click **Become Primary Contact** to update the current contact for the installed package to your username. This contact name displays for the package publisher from the Push Package Upgrade page. Initially, it's set to the name of the person who installed the package. If you have Download AppExchange Packages permission and aren't the current primary contact, this option is enabled.
- Click **Configure** if the publisher has included a link to an external website with information about configuring the package.
- Click the package name to view details about this package.
- View the publisher of the package.
- View the status of the licenses for this package. Available values include:
 - Trial
 - Active
 - Suspended
 - Expired
 - Free

This field is only displayed if the package is managed and licensed.

- Track the number of licenses available (**Allowed Licenses**) and the number of licenses that are assigned to users (**Used Licenses**).
- View the date your licenses for this package are scheduled to expire.
- View the date your licenses were installed.
- View the number of custom apps, tabs, and objects this package contains.
- See whether the custom apps, tabs, and objects count toward your organization's limits. If they do, the box in the **Limits** column is checked.

EDITIONS

Available in: Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer Editions**

USER PERMISSIONS

To uninstall packages:

- Download AppExchange Packages

To assign licenses for a managed package:

- Manage Package Licenses

To download or delete the export file for an uninstalled package:

- Download AppExchange Packages

 **Note:** If you have not installed a licensed managed package, the `Publisher`, `Status`, `Allowed Licenses`, `Used Licenses`, and `Expiration Date` fields do not appear.

After an uninstall, Salesforce automatically creates an export file containing the package data, associated notes, and any attachments. When the uninstall is complete, Salesforce sends an email containing a link to the export file to the user performing the uninstall. The export file and related notes and attachments are listed below the list of installed packages. We recommend storing the file elsewhere because it's only available for a limited time after the uninstall completes. Using this list, you can:

- Click **Download** to open or store the export file.
- Click **Del** to delete the export file.

Expired Managed Packages and Sharing Rules

If a criteria-based sharing rule references a field from a licensed managed package whose license has expired, (`expired`) is appended to the label of the field. The field label is displayed in the field dropdown list on the rule's definition page in Setup. Criteria-based sharing rules that reference expired fields aren't recalculated, and new records aren't shared based on those rules. However, the sharing of existing records prior to the package's expiration is preserved.

SEE ALSO:

[View Installed Package Details](#)

[Importing Package Data](#)

View Installed Package Details

View key details about a package installed from AppExchange, such as the number of custom apps, tabs, and objects it uses. You can also assign licenses to users, uninstall the package, and purchase the package.

To access the package detail page, from Setup, enter *Installed Packages* in the `Quick Find` box, select **Installed Packages**, and then click the name of the package that you want to view.

From this page, you can:

- Click **Uninstall** to remove the package and all its components from your Salesforce organization.
- Click **Manage Licenses** to assign available licenses to users in your organization. You can't assign licenses in Lightning Experience. If you need to assign a license, switch to Salesforce Classic.

 **Note:** If you purchased a site license or if the managed package is not licensed, Salesforce assigns licenses to all your users and you can't manage licenses. Your users can use the package as long as they have the appropriate permissions.

- Optionally, click **View Dependencies** and review a list of components that rely on other components, permissions, or preferences within the package.

Viewing Installed Packages

The installed package page lists the following package attributes (in alphabetical order):

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To uninstall packages:

- Download AppExchange Packages

To manage user licenses for an AppExchange package:

- Manage Package Licenses

Attribute	Description
Action	Can be one of two options: <ul style="list-style-type: none"> • Uninstall • Manage Licenses
Allowed Licenses	The total number of licenses you purchased for this package. The value is "Unlimited" if you have a site license for this package. This field is only displayed if the package is managed and licensed.
Apps	The number of custom apps in the package.
Connected Apps	A list of the connected apps that can have access to a user's Salesforce data after the user and the application have been verified.
Description	A detailed description of the package.
Expiration Date	The date that this license expires, based on your terms and conditions. The expiration date is "Does Not Expire" if the package never expires. This field is only displayed if the package is managed and licensed.
Installed Date	The date of the package installation.
Limits	If checked, the package's custom apps, tabs, and objects count toward your organization's limits.
Namespace	The 1- to 15-character alphanumeric identifier that distinguishes a package and its contents from packages of other developers on AppExchange.
Objects	The number of custom objects in the package.
Package Name	The name of the package, given by the publisher.
Publisher	The publisher of an AppExchange listing is the Salesforce user or organization that published the listing. This field is only displayed if the package is managed and licensed.
Status	The state of a package. Available values include: <ul style="list-style-type: none"> • Trial • Active • Suspended • Expired • Free This field is only displayed if the package is managed and licensed.
Tabs	The number of custom tabs in the package.
Used Licenses	The total number of licenses that are already assigned to users. This field is only displayed if the package is managed and licensed.

Attribute	Description
Version Name	The version name for this package version. The version name is the marketing name for a specific release of a package. It is more descriptive than the Version Number .

Viewing Installed Package Details

The installed package detail page lists the following package attributes (in alphabetical order):

Attribute	Description
Apps	The number of custom apps in the package.
Description	A detailed description of the package.
First Installed Version Number	The first installed version of the package in your organization. This field is only displayed for managed packages. You can reference this version and any subsequent package versions that you have installed. If you ever report an issue with a managed package, include the version number in this field when communicating with the publisher.
Installed By	The name of the user that installed this package in your organization.
Limits	If checked, the package's custom apps, tabs, and objects count toward your organization's limits.
Modified By	The name of the last user to modify this package, including the date and time.
Namespace	The 1- to 15-character alphanumeric identifier that distinguishes a package and its contents from packages of other developers on AppExchange.
Objects	The number of custom objects in the package.
Package Name	The name of the package, given by the publisher.
Package Type	Indicates whether the package is managed or unmanaged.
Post Install Instructions	A link to information on configuring the package after it's installed. As a best practice, the link points to an external URL, so you can update the information independently of the package.
Publisher	The publisher of an AppExchange listing is the Salesforce user or organization that published the listing. This field is only displayed if the package is managed and licensed.
Release Notes	A link to release notes for the package. As a best practice, link to an external URL, so you can make the information available before the release and update it independently of the package.
Tabs	The number of custom tabs in the package.

Attribute	Description
Version Name	The version name for this package version. The version name is the marketing name for a specific release of a package. It is more descriptive than the Version Number.
Version Number	The version number for the latest installed package version. The format is <i>majorNumber.minorNumber.patchNumber</i> , such as 2.1.3. The version number represents a release of a package. The Version Name is a more descriptive name for the release. The <i>patchNumber</i> is generated only when you create a patch. If there is no <i>patchNumber</i> , it is assumed to be zero (0).

Unused Components

You can see a list of components deleted by the developer in the current version of the package. If this field is part of a managed package, it's no longer in use and is safe to delete unless you've used it in custom integrations. Before deleting a custom field, you can keep a record of the data from Setup by entering *Data Export* in the *Quick Find* box, then selecting **Data Export**. After you've deleted an unused component, it appears in this list for 15 days. During that time, you can either undelete it to restore the field and all data stored in it, or delete the field permanently. When you undelete a field, some properties on the field are lost or changed. After 15 days, the field and its data are permanently deleted.

The following component information is displayed (in alphabetical order):

Attribute	Description
Action	Can be one of two options: <ul style="list-style-type: none"> • Undelete • Delete
Name	Displays the name of the component.
Parent Object	Displays the name of the parent object the component is associated with. For example, a custom object is the parent of a custom field.
Type	Displays the type of component.

Package Components

You can see a list of the components included in the installed package. The following component information is displayed (in alphabetical order):

Attribute	Description
Action	Can be one of two options: <ul style="list-style-type: none"> • Undelete • Delete
Name	Displays the name of the component.

Attribute	Description
Parent Object	Displays the name of the parent object the component is associated with. For example, a custom object is the parent of a custom field.
Type	Displays the type of component.

SEE ALSO:

- [Importing Package Data](#)
- [Manage Installed Packages](#)

Importing Package Data

When you uninstall an AppExchange package, Salesforce automatically creates an export file containing the package data as well as any associated notes and attachments. If you choose to install the package again, you can import this data.

Important: Where possible, we changed noninclusive terms to align with our company value of Equality. We maintained certain terms to avoid any effect on customer implementations.

To import your AppExchange package data, use one of the following tools that is available for your Edition:

- For Group Edition, use the appropriate import wizard.
- For Professional Edition, use the appropriate import wizard or any compatible Salesforce ISV Partner integration tool.
- For Enterprise, Developer, Performance, and Unlimited Edition, use the Data Loader.

Notes on Importing AppExchange Package Data

- Salesforce converts date fields into date/time fields upon export. Convert the appropriate fields into date fields before you import.
- Salesforce exports all date/time fields in Greenwich Mean Time (GMT). Before importing these fields, convert them to the appropriate time zone.
- The value of auto number fields may be different when you import. To retain the old values, create a new custom auto number field on a custom object before importing the data.
- Salesforce updates system fields such as `Created Date` and `Last Modified Date` when you import. To retain the old values for these fields, contact Salesforce support.
- Relationships are not included in the export file. Recreate any master-detail or lookup relationships after importing your data.
- Record type IDs are exported but not the record type name.
- Field history is not exported.
- Recreate any customizations that you made to the package after installation.

SEE ALSO:

- [View Installed Package Details](#)
- [Manage Installed Packages](#)

EDITIONS

Available in: both Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

To import Salesforce AppExchange package data:

- The permissions required to use the import tool you choose, such as the import wizard or Data Loader.

Managing Licenses for Installed Packages

When you install a licensed managed package in your organization from AppExchange, you purchase a certain number of licenses from the package developer or publisher. You can assign each license to a user within your organization. If you assign all available licenses, but would like to grant licenses to additional users, you can reassign a license or purchase more. To get more licenses, contact the publisher of the managed package.

Note: If you purchased a site license or if the managed package is not licensed, Salesforce assigns licenses to all your users and you can't manage licenses. Your users can use the package as long as they have the appropriate permissions.

1. From Setup, enter *Installed Packages* in the Quick Find box, then select **Installed Packages**.
2. Click **Manage Licenses** next to the package. To assign licenses for a package, you must have access to the package and at least one available license.
 - a. To assign licenses to more users, click **Add Users**.
 - b. To remove a license from a user, click **Remove** next to the user's name. To remove licenses from multiple users, click **Remove Multiple Users**.
 - c. Click any column heading to sort the users in ascending order using the data in that column. Click the heading again to sort in descending order.
 - d. If available, select **fewer** or **more** to view a shorter or longer display list.

SEE ALSO:

- [Assign Licenses for Installed Packages](#)
- [Removing Licenses for Installed Packages](#)
- [Responding to License Manager Requests](#)

Namespace Permission Set Licenses in Packages

If you install a managed package that has an associated namespace permission set license, you can use it to entitle users access to one or more packages in that namespace. Namespace permission set licenses function in a similar way to managed package licenses.

Namespace permission set licenses appear on the Company Information page along with other permission set licenses. You assign them in the same manner as other permission set licenses. You can entitle access to an entire package or multiple packages, respectively, within a single namespace.

To view the properties and permissions of your namespace permission set license, from Setup, in the Quick Find box, enter *Users*, and then select **Users**. Select a user and from the Permission Set License Assignments related list, click **Edit Assignments**. Here you can view the contents of a permission set license, the package namespace, and license expiration policy details.

Permission Set License	Enabled	Description	Properties and Permissions
Global Traffic Finder	<input checked="" type="checkbox"/>	Entitles users to access the GlobalTraffic namespace.	Package Namespace <ul style="list-style-type: none"> • GlobalTraffic License Expiration Policy <ul style="list-style-type: none"> • Allow Package Access Custom Permissions <ul style="list-style-type: none"> • Global Traffic User

Save Cancel

EDITIONS

Available in: Salesforce Classic (not available in all orgs)

Available in: **Group, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To manage licenses for a AppExchange package:

- Manage Package Licenses

EDITIONS

Available in: Salesforce Classic (not available in all orgs) and Lightning Experience

The availability of each permission set license depends on the edition requirements for permission sets and the related feature.

License Expiration Policy indicates whether package access is blocked for existing users when all namespace permission set licenses expire.

 **Note:** You can assign a permission set unconstrained by licenses that has components from a managed package. If you assign such a permission set, at assignment time Salesforce validates whether the user has a namespace permission set license for the relevant managed package namespace. If users don't have the license, the permission set assignment fails.

Assign Licenses for Installed Packages

If you purchased a site license or if the managed package isn't licensed, Salesforce assigns licenses to all your users and you can't manage licenses. Your users can use the package as long as they have the appropriate permissions.

To assign licenses to specific users:

1. From Setup, enter *Installed Packages* in the **Quick Find** box, then select **Installed Packages** to find the installed package that has available licenses.
2. Click the **Manage Licenses** link next to the package name.
3. Click **Add Users**.
4. Choose a view from the dropdown list, or click **Create New View** to build a new custom view.
5. Select a letter to filter the users with a last name that corresponds with that letter or click **All** to display all users who match the criteria of the current view.
6. Select users.
 - a. To select individual users, use the checkboxes. Selected users are listed in the Selected list. When the list includes all users to which you want to assign licenses, click **Add**.
 - b. To select all users for the current view, click **Add All Users** then click **OK**.
7. (Optional) Certain managed packages created by Salesforce, require external access to data within your org. To grant access to allow an installed managed package to connect with external data, click **Enable for Platform Integrations**. Alternatively, to revoke access between an installed managed package and external data, click **Disable for Platform Integrations**. Enable this functionality only upon request from a Salesforce-owned managed package.

EDITIONS

Available in: Salesforce Classic (not available in all orgs)

Available in: **Group, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To manage licenses for an AppExchange app:

- **Manage Package Licenses**

SEE ALSO:

[Managing Licenses for Installed Packages](#)

Removing Licenses for Installed Packages

You can remove licenses to an AppExchange package from multiple users.

1. From Setup, enter *Installed Packages* in the **Quick Find** box, then select **Installed Packages**.
2. Click **Manage Licenses** next to the package name.
3. Click **Remove Multiple Users**.
4. To show a filtered list of items, select a predefined list from the **View** drop-down list, or click **Create New View** to define your own custom views.
5. Click a letter to filter the users with a last name that corresponds with that letter or click **All** to display all users who match the criteria of the current view.
6. Select users.
 - To select individual users, use the checkboxes. Selected users appear in the Selected for Removal list. When the list includes all users for which you want to remove licenses, click **Remove**.
 - To select all users in the current view, click **Remove All Users**, then click **OK**.

You can also remove licenses for an AppExchange package from a single user using the following options:

1. From Setup, enter *Users* in the **Quick Find** box, then select **Users** and click **Remove** next to the package in the managed packages list.
2. From Setup, enter *Installed Packages* in the **Quick Find** box, then select **Installed Packages**. Then, click **Manage Licenses** next to the package name, and click **Remove** next to the user.

SEE ALSO:

[Managing Licenses for Installed Packages](#)

Responding to License Manager Requests

A license manager is a Salesforce org that tracks all Salesforce subscribers installing a particular AppExchange package.

Salesforce administrators can choose to designate another org as the license manager for one of their packages. The license manager does not need to be the same org as the one from which the package is managed. To choose another org as the license manager, all you need is an email address (not a Salesforce username). If a Salesforce administrator selects to have a third-party license manager and enters your email address, you will receive a license management request in email.

To respond to a registration request:

1. Click the link in the license management request email. This displays the registration request in the requestor's Developer Edition org.
2. Click **Accept** to complete the registration process. Alternatively, click **Reject** to decline the request and close the browser; this prevents you from using the link again. If you accept the request, you authorize Salesforce to automatically create records in your Salesforce org to track information about this package. Choosing a license manager org is permanent and can't be changed.
3. Enter the username and password for the Salesforce org you want to use to manage licenses for this package. A license manager can be any Salesforce org that has installed the free License Management Application (LMA) from AppExchange.

EDITIONS

Available in: Salesforce Classic (not available in all orgs)

Available in: **Group, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To manage licenses for an AppExchange package:

- Manage Package Licenses

USER PERMISSIONS

To respond to registration requests:

- Customize Application

4. Click **Confirm**.

SEE ALSO:

[Managing Licenses for Installed Packages](#)

Assigning Licenses Using the API

Administrators can use the API to assign or revoke licenses for any managed package installed in their organization.

License information for a package is stored in two objects, PackageLicense and UserPackageLicense, which were previously accessible only from the Manage Licenses page under Setup. These are now accessible as standard objects, so an administrator can assign licenses to specific users via API calls. This makes managing package licenses in a subscriber organization faster and easier, especially for large-scale deployments.

For example, suppose an administrator installs an app for use by all 200 salespeople in the company. Assigning a license to each salesperson from the UI is inefficient and time-consuming. Using the API, the administrator can assign licenses to all salespeople, based on their profile, in one step.

Here are some common licensing tasks that administrators can use the API to do.

- Determine the number of package licenses in use and available.
- Verify if a specific user has a license for the package.
- Get a list of all users who have a license for the package.
- Assign a package license to a user or group of users.
- Revoke a package license that was previously assigned to a user.

For details of the PackageLicense and UserPackageLicense objects and a code sample, see the [Object Reference for Salesforce and Lightning Platform](#).

Package Usage

Discover whether your company is taking advantage of AppExchange packages that you installed by reviewing usage summaries. Usage summaries are available for managed packages that passed security review. Usage summaries provide a monthly aggregate view on how your users interacted with these packages. Events from sandbox, scratch, and trial orgs aren't tracked in package usage summaries.

From Setup, in the Quick Find box, enter *Package Usage*, and then select **Package Usage**.

To request a .csv file of your managed package usage data, click **Request Summary**.

To access the link to download your usage summary, refresh the Package Usage page.

The link to download a requested usage summary expires after 15 minutes.

Unauthorized Managed Packages

To participate in the AppExchange Partner Program, Salesforce's partners must meet certain standards and submit their AppExchange products for security review. When you install a managed package that the AppExchange Partner Program hasn't authorized for distribution, we notify you during installation.

EDITIONS

Available in: Salesforce Classic (not available in all orgs)

Available in: **Group, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

USER PERMISSIONS

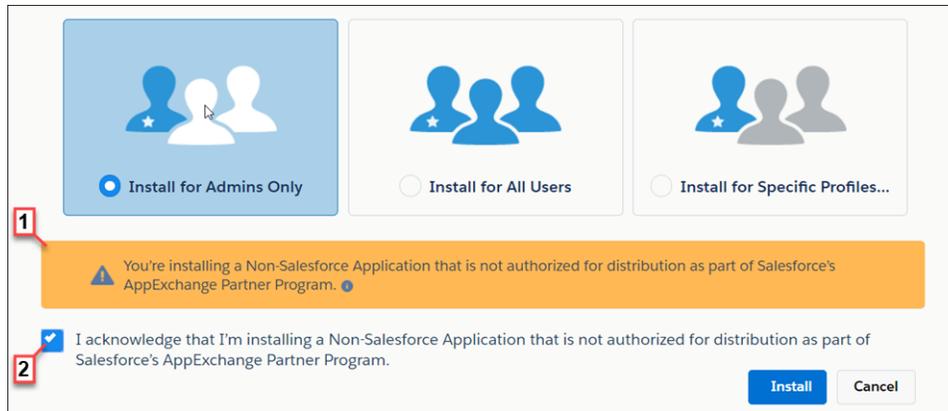
To manage licenses for an AppExchange app:

- Manage Package Licenses

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited, and Developer** Editions



The notification appears when you configure the package installation settings (1). Before you install the package, you must confirm that you understand that the package isn't authorized for distribution (2).

For information about the AppExchange Partner Program and its requirements, visit the [Salesforce Partner Community](#). For information about non-Salesforce providers, see our [Main Services Agreement](#).

SEE ALSO:

[Second-Generation Managed Packaging Developer Guide: Package Usage Summary Schema](#)

Upgrading Packages

Salesforce supports upgrades for managed packages only. Publishers can publish an upgrade for a managed package and notify installers that the new version is available.

Installers of a managed package can then install the upgrade as follows:

1. Before you install an upgrade, determine if the app you installed was from a managed package. Look for the  Managed - Installed icon on the detail pages for each component and on the list of packages installed.

If the app you installed is not from a managed package, upgrades for it are not available.
2. Then, install the upgrade in the same way you would install any other package from the AppExchange. If the publisher provided a link to the new version, follow the link to the package posting and install it in your organization. The first page of the install wizard lists the current version you have installed, the version you're about to install, and a list of additional components included in the new version.

Notes on Upgrading Managed Packages

Consider the following when upgrading a managed package:

- All existing custom objects that were previously deployed will still be deployed. Salesforce prompts you to deploy any new custom objects or previously undeployed custom objects.
- Profile settings for components in a package are editable by the customer but not upgradeable by the package developer. If the developer makes changes to any profile settings after releasing the package, those changes won't be included in an upgrade. Customers will need to manually update the profile settings after upgrading the package. In contrast,

EDITIONS

Available in: Salesforce Classic (not available in all orgs)

Available in: **Group, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To upload packages:

- Upload AppExchange Packages

To install and uninstall packages:

- Download AppExchange Packages

permission sets in a package are upgradeable by the developer, so any changes the developer makes will be reflected in the customer organization after upgrading the package.

- If the developer chooses to add universally required custom fields, the fields will have default values.
- Translation Workbench values for components that are “editable but not upgradeable” are excluded from upgrades.
- If an installed package has `Restricted` API access, upgrades are successful only if the upgraded version does not contain any s-controls. If s-controls are present in the upgraded version, you must change the currently installed package to `Unrestricted` API access.
- When you upgrade a package, changes to the API access are ignored even if the developer specified them. This ensures that the administrator installing the upgrade has full control. Installers should carefully examine the changes in package access in each upgrade during installation and note all acceptable changes. Then, because those changes are ignored, the administrator should manually apply any acceptable changes after installing an upgrade.

SEE ALSO:

[ISVforce Guide: Use Managed Packages to Develop Your AppExchange Solution](#)

Installing Packages FAQ

Find answers for frequently asked questions about installing packages.

- [Can I uninstall packages that I installed from AppExchange?](#)
- [Who Can Use AppExchange?](#)
- [Why did my installation or upgrade fail?](#)
- [Can I customize AppExchange packages?](#)
- [Who can use AppExchange packages?](#)
- [How can I upgrade an installed package?](#)
- [How secure are the components I install?](#)
- [What happens to my namespace prefix when I install a package?](#)
- [Can I reinstall an AppExchange package after uninstalling it?](#)
- [When I install a package that’s listed on AppExchange, do custom objects, custom fields, tabs, and apps in the package count against the limits of my Salesforce edition?](#)

EDITIONS

Available in: Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: **Essentials, Group, Professional, Enterprise, Performance, Unlimited,** and **Developer** Editions

Can I uninstall packages that I installed from AppExchange?

Yes. All your installed packages are listed in the Installed Packages page. You can remove any package by clicking the **Uninstall** link next to the package name.

SEE ALSO:

[Uninstall a Managed Package](#)

[Importing Package Data](#)

Who Can Use AppExchange?

Anyone can browse and test drive AppExchange listings.

Salesforce admins and users with the Download AppExchange Packages permission can install AppExchange apps. To publish a listing on AppExchange, a user needs both Create AppExchange Packages and Upload AppExchange Packages permissions.

Why did my installation or upgrade fail?

An installation can fail for several reasons.

- The package includes custom objects that cause your organization to exceed its limit of custom objects.
- The package includes custom tabs that cause your organization to exceed its limit of custom tabs.
- The developer of the package has uploaded a more recent version of the package and has deprecated the version associated with this installation URL. Contact the publisher of the package to get the most recent installation URL.
- You're trying to install an extension to a package, and you don't have the base package installed.
- The package requires that certain components are enabled in your organization, or that required features are enabled in your edition.
- The package contains Apex code and you are not authorized to run Apex in your organization.
- The package you're installing has a failing Apex test.

Can I customize AppExchange packages?

Yes, all packages are customizable. However, to ensure compatibility with future versions, some aspects of managed packages can't be changed.

For a list of components that are editable in a managed package, see [Components Available in Managed Packages](#) in the *Second-Generation Managed Packaging Developer Guide*.

Who can use AppExchange packages?

If you use an Enterprise, Unlimited, Performance, or Developer Edition organization, you can choose which user profiles have access to the package as part of the installation process.

Packages installed in Professional and Group Edition organizations are installed with "Full Access" to all user profiles. However, regardless of Edition, all custom objects are installed in "In Development" mode, which hides them from all standard users. Users must have the "Customize Application" permission to view custom objects in "In Development" mode. When you are ready to roll out the package to other users, change the custom object status to "Deployed."

How can I upgrade an installed package?

Managed packages are completely upgradeable. Before installing a package, contact the publisher to determine if it's managed.

How secure are the components I install?

Salesforce performs periodic security reviews of all publicly listed applications on AppExchange. When installing third party applications with access to data, these applications have access to other data within the organization where the package was installed.

Private listings don't go through a security review and administrators must inspect the application carefully before determining whether to install it within their organization.

What happens to my namespace prefix when I install a package?

A namespace prefix is a globally unique identifier that you can request if you plan to create a managed package.

All the components from a managed package that you install from another developer contain the developer's namespace prefix in your organization. Unmanaged packages can have a namespace prefix while they're developed in an org that contains a managed package. This namespace isn't used outside of the development (publisher) org. If an unmanaged package is installed in an org that has no

namespace, then the unmanaged components have no namespace in the subscriber org. If an unmanaged package is installed in an org that has a namespace, then the components get the namespace of the subscriber org.

Can I reinstall an AppExchange package after uninstalling it?

Yes. You can reinstall a package in the same manner that you installed it.

SEE ALSO:

[Install a Package](#)

[Importing Package Data](#)

When I install a package that's listed on AppExchange, do custom objects, custom fields, tabs, and apps in the package count against the limits of my Salesforce edition?

Your Salesforce edition is allocated a certain number of custom objects, custom fields, tabs, and other customizations. At the same time, all Salesforce orgs have a total limit on some of these items.

If you install a package from AppExchange, its custom objects, custom fields, tabs, and apps don't count against your edition's allocation, but they do count against the total limit of your Salesforce org.

These rules apply only to managed packages that are listed on AppExchange. If you install an unmanaged package or a managed package that's not publicly listed on AppExchange, its custom objects, custom fields, tabs, and apps count against the allocation for your Salesforce edition.

If you have an AppExchange managed package installed in your org and the status of that package is expired or suspended, custom fields in that package are no longer excluded from the org's Salesforce edition custom field limit and count against that custom field limit. To fix this issue, reactivate your license or uninstall the package.

Do AppExchange managed packages count against data storage limits?

Yes. Data stored in the records associated with custom objects in managed packages, count against your org's data storage limits.

Learn More About Setting Up Salesforce

In addition to online help, Salesforce creates guides and tip sheets to help you learn about our features and successfully administer Salesforce.

Data Import

Guides and Tip Sheets	For End Users	For Admins
Data Loader Guide		✓
Using Mass Delete to Undo Imports		✓

Data Management

Guides and Tip Sheets

For End Users**For Admins**[Salesforce Field Reference Guide](#)

Security

Guides and Tip Sheets

For End Users**For Admins**[Security Implementation Guide](#)[Salesforce Identity Connect 3.0.1 Release Notes and Implementation Guide](#)[Platform Encryption Implementation Guide](#)[Understanding User Sharing](#)[Understanding Defer Sharing Calculations](#)

INDEX

A

Activities
 controlled by parent [595](#)
apex [1103](#)
Apex classes [1097](#), [1102](#)
api event [1079](#)
attachments [935](#)

B

background encryption [966–968](#), [970](#)
baseline [889](#)
best practices for Shield Platform Encryption [1001](#)
Bring Your Own Key (BYOK) [943](#), [974–977](#), [980](#), [982](#)
Browser security [1038](#)

C

Cache-Only Key [982–984](#), [986](#), [991–994](#)
Certificates
 api client [1210](#)
 mutual authentication [1209–1210](#)
 uploading [1209](#)
compatibility [958](#)
condition [1079](#), [1082](#), [1085](#)
Condition Builder [1075](#), [1079](#), [1082](#), [1085](#), [1090](#)
conditions [1079](#), [1082](#), [1085](#)
considerations [993](#), [1000](#), [1008](#), [1011–1012](#)
custom fields [934](#), [952](#)
customizations [997](#)

D

data encryption [921–922](#), [934–935](#), [952](#)
Data Loader
 blank fields, replacing [720](#)
 updating fields with blank values [720](#)
data visibility [944](#)
definitions [984](#)
deploy [945](#)
destroy key material [970](#), [973](#), [992](#)
deterministic encryption [959–960](#), [1008](#)

E

encryption policy [921](#), [946](#), [952](#)
encryption process [937](#), [940](#)
encryption statistics [966–968](#)
enhanced transaction security [1103](#)

export key material [966](#)
Exporting
 from LinkedIn [687](#)

F

FAQ
 importing or uploading data [715](#)
 mass upload [715](#)
 replacing fields with blank values [720](#)
 updating fields with blank values [720](#)
 what data can be imported [716](#)
field limits [1012](#)
fields [922](#)
Fields
 sharing model [595](#)
files [935](#)
formulas [998](#)

G

Getting started
 mass upload [715](#)

H

health check [889](#)
High assurance [1040](#)
History
 disabling field tracking [1244](#)

I

Import wizards
 Data Import Wizard [717–718](#), [721](#)
Importing
 data [716](#)
 Data Import Wizard [717–718](#), [721](#)
 importing or uploading data [715](#)
 person accounts [704](#)

K

key management [963–964](#), [966–968](#), [970](#), [973](#), [976–977](#), [980](#), [986](#)
key material [949](#)
Key pairs [1206](#)

L

Lightning Experience [1011](#)
LinkedIn
 exporting data [687](#)

Login
 activations [1060–1061](#)
 browser security [1038](#)
 identity verification [1060](#)
login event [1082, 1085](#)
login forensics
 considerations [1232](#)
Login Forensics
 enable [1233](#)
Logout events
 LogoutEventStream [1072](#)
LogoutEventStream
 logout events [1072](#)

M

masking [944](#)
Master encryption keys [1206](#)
monitoring [1223](#)
multi-factor authentication [973](#)

N

Network access [1060–1061](#)

O

Organization-wide sharing settings
 standard report visibility [642](#)

P

Permission set groups
 permission sets [566](#)
 recalculation [565](#)
policies [1075, 1079, 1082, 1085, 1090](#)
prerequisites [984](#)

R

real time events [1075, 1079, 1082, 1085, 1090](#)
real-time events [1061–1065, 1068, 1070, 1073, 1075, 1079, 1082, 1085, 1090, 1126, 1128–1132, 1134, 1136–1140, 1142–1143](#)
Rotating master encryption keys [1206](#)

S

sandbox [943](#)
Scheduled jobs
 about [1254](#)
 viewing [1254](#)
script for BYOK key [977](#)
search index [942](#)
Security
 Apex policy classes examples [1097, 1102](#)

Security (*continued*)
 auditing [895](#)
 certificates [1206](#)
 creating [1075, 1079, 1082, 1085, 1090](#)
 enhanced transaction security implementation examples
 [1097, 1102](#)
 identity verification activations [1060–1061](#)
 key pair [1206](#)
 master encryption keys [1206](#)
 overview [879](#)
 queues [581](#)
 session [1031](#)
 SSL [1031](#)
 timeout [1031](#)
 TLS [1031](#)
 transaction security policies [1075, 1079, 1082, 1085, 1090](#)
security check [889](#)
security risk [889](#)
Session security [1040](#)
Sharing
 Grant data access using hierarchies [598](#)
 organization-wide sharing settings [595](#)
State and country picklists
 converting data overview [326](#)
synchronize data [967, 970](#)

T

Team
 See Account team [581](#)
 See Case teams [581](#)
tenant secret [949, 963–964](#)
terminology [984](#)
testing [1103](#)
threat detection [1126, 1128–1132, 1134, 1136–1140, 1142–1143](#)
Training history [1234](#)
transaction security [1075, 1079, 1082, 1085, 1090, 1097, 1102](#)
troubleshoot Bring Your Own Key [980](#)
troubleshoot Cache-Only Key [991, 994](#)
troubleshoot Shield Platform Encryption [958](#)
two-factor authentication [973](#)

U

Updating
 blank values [720](#)
User Sharing
 compatibility with report types [639](#)
Users
 usage-based entitlements [467](#)

V

validation service [958](#)