Set Up and Maintain Collaboration Tools

Salesforce, Spring '24

'24

CONTENTS

SET UP AND MAINTAIN COLLABORATION TOOLS

Help your users collaborate with each other and with people outside your organization. For help with basic Salesforce administration, see Set Up Your Organization.

Salesforce Chatter

Connect, engage, and motivate users to collaborate and work efficiently across the organization regardless of their role or location.

Salesforce Files

Customize page layouts to include the Files related list, so users see a list of files associated with a record.

Salesforce Files Connect

With Files Connect, Salesforce users can access, share, and search external data from systems like Quip, Google Drive, SharePoint, or Box.

Salesforce CRM Content

Store, share, and manage your files in content libraries.

Google Apps

Enable Google apps like Google Docs, Gmail, and Google-related AppExchange apps—customized for use within Salesforce.

Collaboration Resources for Admins

In addition to online help, Salesforce publishes printable documentation to help you learn about our features and successfully administer Salesforce.

Salesforce Chatter

Connect, engage, and motivate users to collaborate and work efficiently across the organization regardless of their role or location.

Salesforce Chatter lets users collaborate on sales opportunities, service cases, campaigns, and projects with embedded apps and custom actions. By default, Salesforce organizations created after June 22, 2010 have Chatter already enabled for all users. However, if you want Chatter to be available to a limited group of people in your org, you can do a profile-based rollout instead.

With a profile-based rollout, only users who have been assigned the required user profile or permission set have access to Chatter. A profile-based rollout is useful for larger companies and companies or government agencies with regulatory constraints. It allows such orgs to plan a controlled deployment on a department-by-department basis.

Although we recommend an org-wide Chatter deployment, the option to limit its availability is there. Ask Salesforce about enabling a profile-based Chatter rollout. Chatter is secure and works in accordance with all the security and permission settings in your Salesforce organization.

Profile-Based Chatter Rollout Overview

A profile-based rollout of Chatter makes Chatter available to a controlled set of users instead of all users in your organization.

EDITIONS

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

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

USER PERMISSIONS

To enable Chatter:
- Customize Application

Encryption for Chatter

Encryption for Chatter lets you encrypt sensitive data when it's stored, and not just when it's transmitted over a network. As of the Winter '18 release, mass encryption and decryption of Chatter data is generally available. To enable encryption for Chatter, contact support for help with setting it up.

Chatter Settings

In Salesforce and the Salesforce mobile app, Chatter is enabled by default. Configure various Chatter features and customize the Chatter experience for your users on the Chatter Settings page in Setup.

Publisher Actions and Layouts

Actions add functionality to the Chatter Publisher in Salesforce Classic. Actions let your users do more in Salesforce across all devices.

Enable Code Snippets and Assign Permissions to Use Them

Use code snippets to enter syntax-highlighted code samples through the Chatter publisher. To make code snippets available, enable them and assign the permission to use them. There are two ways to enable code snippets and assign permission: through a user profile (step 1) or through a permission set (step 2). Code snippets are available in Lightning Experience and Experience Builder sites that are based on the Customer Service template.

Assign Pin Post Permission

Pin your most critical information to the top of a feed. In group and topics feeds, an authorized user can pin up to three posts. A pinned post stays in place until an authorized user unpins it. After you enable post pinning through Chatter Settings, you can assign the Pin Posts in Feeds permission through a permission set or a user profile.

Feed Tracking

Feed tracking detects changes to tracked record fields and posts them as updates in the What I Follow feed. Users who follow a record, see those updates in their view of What I Follow, with one exception. Updates users make themselves aren't posted to What I Follow. Users can see those updates in their profile feeds.

Chatter Email Settings and Branding

Chatter email settings let you change the format of your company's outgoing emails and control whether users receive email notifications.

Chatter Post Actions and Layouts

Actions on posts and comments appear in the drop-down menu on a post or comment. Users can edit, bookmark, mute, and delete posts, add topics, and create tasks from posts.

Group Layouts

The group layout lets you customize which fields, buttons, actions, and lists appear in Chatter groups. Changes to the group layout affect all groups in your organization, but they appear only on the group pages in the Salesforce mobile app. Changes to the group publisher appear in both the full Salesforce site and the Salesforce mobile app.

Topics for Objects

Topics for objects offers a powerful way to crowdsource your company's key themes and issues. Users can add topics to records to organize them by common themes.

Customize Chatter Influence

Customize activity thresholds for posts, comments, and likes to improve the Chatter influence calculation.

Allow Users to Thank Their Coworkers

Recognize your coworkers with thanks badges and post your thanks directly to the Chatter feed.

Guidelines for Deleting Your Users' Chatter Messages

Salesforce administrators with the Manage Chatter Messages permission can access all users' private messages via SOAP API. You can view and delete any message (for example, for compliance).

Report on Chatter with the Dashboards Package

The Chatter Dashboards package for Salesforce Classic packs a punch! You get multiple dashboards, over 100 reports, and even custom report types. Use the dashboards to monitor and manage Chatter adoption and engagement in your organization.

Chatter Desktop

Control access to Chatter Desktop and install and configure the Chatter Desktop Managed Version.

Profile-Based Chatter Rollout Overview

A profile-based rollout of Chatter makes Chatter available to a controlled set of users instead of all users in your organization.

Once profile-based rollout is enabled for your organization, you can enable Chatter for the users with the required user profile or permission sets. Users without the right profile or permission set don't have access to Chatter.

👁 **Example:** Let's say you assign a profile or permission set that excludes Chatter access to a subset of users. These users still have access to Salesforce objects, but they don't see the record feed and they can't post or comment.

Get Ready for Profile-Based Rollout of Chatter

If you're rolling out Chatter to a subset of your users, you can manage Chatter access with custom user profiles and permission sets. There's a little up-front work you can do to prepare.

Control Chatter Access Through User Profiles

Modify existing custom user profiles to allow or deny access to Chatter.

Control Chatter Access Through Permission Sets

Manage Chatter access by modifying existing permission sets or setting up new ones.

Profile-Based Rollout Considerations

In organizations that use Chatter profile-based rollout, limitations apply. There are limits with user profiles, permissions sets, and the interaction between users with and without Chatter access.

Get Ready for Profile-Based Rollout of Chatter

If you're rolling out Chatter to a subset of your users, you can manage Chatter access with custom user profiles and permission sets. There's a little up-front work you can do to prepare.

From a high-level perspective, a profile-based rollout of Chatter consists of these steps:

📝 **Note:** Before you begin, disable Chatter for your entire organization (in Setup, go to Chatter settings and deselect **Enable**).

1. Salesforce enables the Chatter profile-based rollout feature for your organization.

2. You determine who gets access to Chatter.

3. You review and modify existing custom user profiles and permissions sets.

4. Verify that, in a custom user profile or permission set, the Enable Chatter,permission has the desired setting.

5. To allow or restrict Chatter access, assign the associated profile or permission set to users.

6. You turn on Chatter for your organization.

> **Note:** Perform step 6 as a separate, final step. If step 6 is combined with another step or performed out of order, unpredictable and undesirable results can occur.

SEE ALSO:

Profile-Based Chatter Rollout Overview

Control Chatter Access Through User Profiles

Control Chatter Access Through Permission Sets

Control Chatter Access Through User Profiles

Modify existing custom user profiles to allow or deny access to Chatter.

When Salesforce turns on Chatter profile-based rollout for your organization, it adds the Enable Chatter permission to your existing user profiles and permissions sets. Enable Chatter is automatically enabled for all standard profiles. It's also automatically enabled for custom profiles when any of these user-level permissions are enabled manually or as part of a license:

- Create and Own New Chatter Groups (ChatterOwnGroups)—Users with this permission can create groups in Chatter.
- Create and Share Content Deliveries for Chatter Files (ChatterFileLink)—Users with this permission can use files with Chatter, like uploading, attaching, and sharing.
- Invite Customers To Chatter (ChatterInviteExternalUsers)—Users with this permission can invite users who don't have a Salesforce license to Chatter.
- Manage Chatter Messages and Direct Messages (ManageChatterMessages)—Users with this permission have management access to Chatter Messages and Direct Messages (Experience Builder sites).
- Moderate Chatter (ModerateChatter)—Users with this permission can moderate Chatter feeds.
- Moderate Chatter Feeds (ModerateNetworkFeeds)—Users with this permission can moderate feeds in sites.
- Use Case Feed (ViewCaseInteraction)—Users with this permission can access Case feeds.
- View All Data (ViewAllData)—Users with this permission can view all data, regardless of their membership status in a feed or ownership of a record.

Modify your existing custom profiles with the desired permissions to manage access to Chatter, and create custom profiles, if necessary.

1. Log in as a Salesforce administrator.

2. From Setup, enter *Profiles* in the `Quick Find` box, then select **Profiles**.
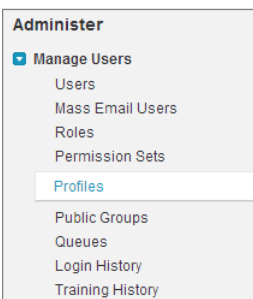
EDITIONS

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

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

USER PERMISSIONS

To enable Chatter:
- Customize Application

3. For each custom user profile:

    a. Click **Edit**.

    b. In the Administrative Permissions section, select or deselect **Enable Chatter**, depending on whether you want users with this profile to have Chatter access.

> 🛑 **Important:** The Enable Chatter permission is available only if Chatter profile-based rollout is enabled for your organization. Salesforce enables profile-based rollout at your request. After profile-based rollout is enabled, selecting the Enable Chatter permission on a profile doesn't automatically enable Chatter for people with that profile. People can't use Chatter until you turn on Chatter for your organization.

    c. Save your changes.

4. If applicable, create custom user profiles with the desired permissions and assign them to users.

SEE ALSO:

    Get Ready for Profile-Based Rollout of Chatter

    Control Chatter Access Through Permission Sets

    Chatter Settings

    Profile-Based Rollout Considerations

Control Chatter Access Through Permission Sets

Manage Chatter access by modifying existing permission sets or setting up new ones.

When you enable or disable Chatter through permission sets, consider that:

- When you enable Chatter in a permission set, the permission set takes precedence over user profile settings. All users with a Chatter-enabled permission set have access to Chatter, even if Chatter isn't enabled in their user profile.

- When you disable Chatter in a permission set, the permission set doesn't take precedence over user profile settings. All users with a Chatter-enabled user profile have access to Chatter, even if Chatter is disabled in their permission set. To prevent that person from accessing Chatter, disable Chatter in both the person's user profile and permission set.

- When Chatter profile-based rollout is enabled for an org, Chatter is automatically enabled when some user-level permissions are already enabled. And some Chatter settings are disabled. For more information, see Profile-Based Rollout Considerations on page 8.

Verify that existing permission sets include the correct and required Chatter permissions for the desired subset of users.

1. In Setup, navigate to Permission Sets.

2. For each existing user-level permission set:

   a. In the System section, click **System Permissions**.

   b. Click **Edit**, and select **Enable Chatter**. The Enable Chatter permission is available in a permission set only after Chatter profile-based rollout is enabled for your org.

EDITIONS

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

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

USER PERMISSIONS

To enable Chatter:
- Customize Application

   c.   Save your changes.

3. If applicable, create permission sets with the desired permissions and assign them to users. By default, all permissions in a new permission set are disabled. Enable the appropriate permissions in the new permission set to give users access to Chatter plus extra levels of management authority.

- Create and Own New Chatter Groups (ChatterOwnGroups)—Users with this permission can create groups in Chatter.

- Create and Share Content Deliveries for Chatter Files (ChatterFileLink)—Users with this permission can use files with Chatter, like uploading, attaching, and sharing.

- Invite Customers To Chatter (ChatterInviteExternalUsers)—Users with this permission can invite users who don't have a Salesforce license to Chatter.

- Manage Chatter Messages and Direct Messages (ManageChatterMessages)—Users with this permission have management access to Chatter Messages and Direct Messages (Experience Builder sites).

- Moderate Chatter (ModerateChatter)—Users with this permission can moderate Chatter feeds.

- Moderate Chatter Feeds (ModerateNetworkFeeds)—Users with this permission can moderate feeds in sites.

- Use Case Feed (ViewCaseInteraction)—Users with this permission can access Case feeds.

- View All Data (ViewAllData)—Users with this permission can view all data, regardless of their membership status in a feed or ownership of a record.

> 📝 **Note:** Selecting the Enable Chatter permission in a person's permission set doesn't automatically turn on Chatter for that person. People can't use Chatter until you turn on Chatter for your organization.

SEE ALSO:

Get Ready for Profile-Based Rollout of Chatter

Control Chatter Access Through User Profiles

Chatter Settings

Profile-Based Rollout Considerations

Profile-Based Rollout Considerations

In organizations that use Chatter profile-based rollout, limitations apply. There are limits with user profiles, permissions sets, and the interaction between users with and without Chatter access.

- The Enable Chatter option isn't available on profiles or permission sets unless profile-based rollout of Chatter is enabled for the organization.

- When you enable Chatter in a permission set, the permission set takes precedence over user profile settings. All users with a Chatter-enabled permission set have access to Chatter, even if Chatter isn't enabled in their user profile.

- When you disable Chatter in a permission set, the permission set doesn't take precedence over user profile settings. All users with a Chatter-enabled user profile have access to Chatter, even if Chatter is disabled in their permission set. To prevent that person from accessing Chatter, disable Chatter in both the person's user profile and permission set.

- Enabling Chatter in a person's user profile or permission set doesn't automatically turn on Chatter for the organization. Turn on Chatter for your organization in Setup, after you modify user profiles and permission sets.

- Standard Salesforce user profiles have Chatter enabled by default. You can't disable Chatter for these standard profiles.

- Don't deselect the Enable Chatter permission on a cloned Chatter External user profile. The user sees an error message and can't log in.

- Don't deselect the Enable Chatter permission on a cloned Chatter Free or Chatter Moderator profile. You get an error message and can't save the profile.

- Enabling Chatter and profile-based rollout for an organization also enables a set of dependent Chatter user permissions. If Chatter is disabled for the organization, these permissions are also disabled at the same time. However, if Chatter is reenabled, these permissions aren't automatically re-enabled, and the administrator must enable them explicitly.

- When profile-based rollout of Chatter is enabled for an organization, Chatter is automatically enabled for standard profiles. For custom profiles and permission sets, Chatter is automatically enabled if any of these user-level permissions are enabled manually or as part of a license:

  - Create and Own New Chatter Groups (ChatterOwnGroups)—Users with this permission can create groups in Chatter.

  - Create and Share Content Deliveries for Chatter Files (ChatterFileLink)—Users with this permission can use files with Chatter, like uploading, attaching, and sharing.

  - Invite Customers To Chatter (ChatterInviteExternalUsers)—Users with this permission can invite users who don't have a Salesforce license to Chatter.

  - Manage Chatter Messages and Direct Messages (ManageChatterMessages)—Users with this permission have management access to Chatter Messages and Direct Messages (Experience Builder sites).

  - Moderate Chatter (ModerateChatter)—Users with this permission can moderate Chatter feeds.

  - Moderate Chatter Feeds (ModerateNetworkFeeds)—Users with this permission can moderate feeds in sites.

- – Use Case Feed (ViewCaseInteraction)—Users with this permission can access Case feeds.
  - – View All Data (ViewAllData)—Users with this permission can view all data, regardless of their membership status in a feed or ownership of a record.

- When profile-based rollout of Chatter is enabled for an organization, two org preferences are set to OFF:
  - – Allow Coworker Invitations (inviteCsnUserEnabled)
  - – Allow Customer Invitations (inviteChatterGuestEnabled)

- In organizations that have thanks badges enabled, users with access to Chatter can't thank users who don't have access to Chatter.

- If your organization already has Chatter enabled and switches to profile-based rollout of Chatter, manually enable Chatter in all existing custom profiles and permission sets. Otherwise, users that are assigned these custom profiles and permission sets lose access to Chatter.

- When profile-based rollout of Chatter is enabled in Salesforce Classic, users who can't use Chatter also can't use global search. Advanced search is available to these users.

Encryption for Chatter

Encryption for Chatter lets you encrypt sensitive data when it's stored, and not just when it's transmitted over a network. As of the Winter '18 release, mass encryption and decryption of Chatter data is generally available. To enable encryption for Chatter, contact support for help with setting it up.

Encryption applies to all Chatter feeds. It lets your company comply confidently with privacy policies, regulatory requirements, and contractual obligations for handling Chatter data.

Encrypted fields work normally throughout the Salesforce user interface, business processes, and APIs. (There are some exceptions; for example, encrypted fields can't be filtered.) When you encrypt a field, existing values aren't encrypted immediately. Values are encrypted only after you interact with them, for example, you add or edit field content.

Encrypted fields include:

- Feed posts and comments
- Feed questions and answers
- Link labels and URLs
- Feed polls and poll choices
- Content from your custom Rich Publisher Apps

> **Note:** If you participated in the pilot, turn encryption for Chatter off and on again to include new fields. Contact Salesforce for assistance with encrypting all previously created data.

Enabling encryption for Chatter disables Einstein Spam Detection and exposes Chatter to the global limitations that come with encryption.

EDITIONS

Available in: Salesforce Classic (not available in all orgs), Lightning Experience, and the Salesforce mobile app

Available for an extra cost 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.

Chatter Settings

In Salesforce and the Salesforce mobile app, Chatter is enabled by default. Configure various Chatter features and customize the Chatter experience for your users on the Chatter Settings page in Setup.

- To access the Chatter Settings page in Setup, enter `Chatter` in the `Quick Find` box and select `Chatter Settings`.
- To disable Chatter for your entire organization, deselect `Enable` in the Chatter Settings section.

Chatter Group Settings

Use Chatter group settings to configure group features like group archiving, records in groups, and unlisted groups.

Set the Format of Timestamps on Case Feed Posts

In case feeds show users a relative timestamp on new posts, like 10m ago, or an absolute timestamp, like January 7, 2020 at 12:15PM. Comments and replies are also shown with relative timestamps.

Convert Character Combinations into Emoticons in the Feed

Emoticons let your users enter character combinations in their posts and comments to create expressions.

Let Users Set Out-of-Office Messages in Chatter

Let your users schedule and customize an out-of-office message, and place it next to their name in Chatter. You can enable or disable this feature in Setup, under Chatter Settings. Setting an out-of-office message is available only in Lightning Experience.

Customer Invitations

Let users invite customers to the private groups that they own or manage. Customers are users outside of your company's email domains. They have limited Chatter access and can see only the groups that they're invited to. They can interact only with members of those groups.

Coworker Invitations

Let Salesforce users invite coworkers without Salesforce licenses to Chatter. Invited users can access Chatter people, profiles, groups, and files, but they can't see record data unless they have a Salesforce license.

Enable Add Actions in the Chatter Publisher

In Salesforce Classic, before you can add global actions to the Chatter publisher, you must first enable the Actions in the Publisher feature in Chatter Settings. Actions add functionality to the Chatter publisher and let your users do more in Salesforce across every device.

Feed Post and Comments Editing Overview

With feed post editing, users can edit their own feed posts. Record owners can also edit any post on records they own, no matter who created the post.

SEE ALSO:

Salesforce Chatter

Topics Privacy

Chatter Group Settings

Use Chatter group settings to configure group features like group archiving, records in groups, and unlisted groups.

Available in: both Salesforce Classic and Lightning Experience

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

Chatter Group Archiving
Group archiving is enabled by default for your organization. If a group has no new feed posts or comments for 90 consecutive days, the group is archived automatically. When group archiving is enabled, feed activity in groups is automatically reviewed weekly.

Enable Records in Chatter Groups
By default, records are allowed in groups. But you can also customize the group publisher to include the Add Record action, so users can add records to groups.

Enable Unlisted Chatter Groups
Enable unlisted groups for your organization to help users collaborate more privately in Chatter.

Unlisted Group Limitations
Before you decide to enable unlisted groups in your organization, consider these limitations.

Chatter Group Archiving

Group archiving is enabled by default for your organization. If a group has no new feed posts or comments for 90 consecutive days, the group is archived automatically. When group archiving is enabled, feed activity in groups is automatically reviewed weekly.

Mentioning a group doesn't count as feed activity and doesn't delay group archiving. Archived groups count toward your org's group limits (30,000) but not toward a user's group membership limits (300).

There are more group archiving settings on the group settings page. That's where group owners and managers can archive or activate the group and edit automatic archiving settings. To change archiving settings for multiple groups at once, use the Salesforce API.

If your organization doesn't want to use group archiving, disable this feature in Setup. Enter `Chatter` in the `Quick Find` box, select **Chatter Settings**, and deselect **Allow Group Archiving** in the Groups section.

> **Note:** You can take steps to allow group owners and managers to archive, activate, or disable automatic archiving in the Salesforce mobile app and Lightning Experience. Customize the group layout and add the necessary fields.

SEE ALSO:
Group Layouts

<div style="float:right">

EDITIONS

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

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

</div>

Enable Records in Chatter Groups

By default, records are allowed in groups. But you can also customize the group publisher to include the Add Record action, so users can add records to groups.

The Add Record action on the group publisher lets users add records to groups. Users can add account, contact, lead, opportunity, contract, campaign, case, and custom object records. The **Add Record** action isn't available by default. But you can configure the group publisher to include it.

Consider also customizing object layouts to include the Groups related list on record detail pages. The Groups related list shows users the list of groups that are associated with the record. Customize the layout of all the standard and custom objects in your organization that support group-record relationships.

If you don't want users to add records to groups, enter `Chatter` in the `Quick Find` box in Setup, then select `Chatter Settings`, and deselect **Allow records in groups in the Groups** section. Disabling the feature hides the Group Records list on the group detail page and the **Add Record** action in the group publisher.

For custom objects, you can choose which record types users can add to groups. For each custom object that you want to manage, go to the custom object detail page and, under Optional Features, select **Allow in Chatter Groups**.

> **Note:** Custom object records added to a group before Summer '15, when selecting record types was added, continue to appear in the Group Records list. Be sure to enable this feature for each existing custom object that you want to allow in groups.

SEE ALSO:

Customize the Chatter Group Layout and Publisher

Enable Unlisted Chatter Groups

Enable unlisted groups for your organization to help users collaborate more privately in Chatter.

Unlisted groups offer more privacy compared to private groups. Only group members and users with the Manage Unlisted Groups permission can access unlisted groups in list views, feeds, and search results. By default, unlisted groups aren't enabled for your organization. Review the limitations of unlisted groups, before you enable this feature in your organization.

1. From Setup, enter `Chatter` in the `Quick Find` box, then select **Chatter Settings**.

2. Click **Edit**.

3. Select **Enable Unlisted Groups**.
   A message with important information appears, giving you more detail about enabling unlisted groups in your organization.

4. In the highlighted message, select the checkbox next to **I want to enable unlisted groups and understand that I may need to update Apex/Visualforce code in my organization**.

5. Click **Save**.

Any user can create an unlisted group. Unlike private groups, users with the View All Data or Modify All Data permission can't view or update unlisted groups unless they're members. To allow

non-members to view and modify unlisted groups, assign the Manage Unlisted Groups permission to them via their profile or permission set.

SEE ALSO:

[Unlisted Group Limitations]

Unlisted Group Limitations

Before you decide to enable unlisted groups in your organization, consider these limitations.

For Administrators

- Without membership in an unlisted group, only users with the Manage Unlisted Groups permission can access or modify an unlisted group and its files and feed content.

- Users with the Modify All Data permission can't delete feed content from unlisted groups, unless they are also group members.

- Users with the Data Export permission can export all Chatter data and view the exported posts and comments from any group. They can perform these actions regardless of whether they have the Manage Unlisted Groups permission.

- You can't grant the Manage Unlisted Groups permission to users with these profiles: Chatter External, High Volume Portal, or High Volume Customer Portal.

- Unlisted groups count toward a user's group limit. Even so, unlisted groups don't appear in the Groups list on a user's profile unless the person who's viewing the list is a member or has permission to manage unlisted groups. When unlisted groups are hidden, the count that appears next to the Groups list can be inaccurate, depending on the permissions of the person viewing the list.

For Developers

Apex code runs in system mode, which means that the permissions of the current user aren't taken into account. This limitation has implications for pages that are written in Apex.

- Visualforce pages that display groups can expose unlisted groups to users who aren't members.

- Because system mode disregards the user's permissions, all users who are accessing a Visualforce page that's showing an unlisted group can act as an owner of that group.

- AppExchange apps that are written in Apex and that access all groups expose unlisted groups to users who aren't members.

To limit and manage access to the unlisted groups in your organization:

- In all Apex code, explicitly filter out unlisted groups from SOQL queries.

- Use permission sets, profile-level permissions, and sharing checks in your code to further limit unlisted group access.

- To monitor and manage the creation of unlisted groups, use Apex triggers on the CollaborationGroup object. In Setup, enter `Group Triggers` in the Quick Find box, then select **Group Triggers** to add triggers.

SEE ALSO:

[Enable Unlisted Chatter Groups]

Set the Format of Timestamps on Case Feed Posts

In case feeds show users a relative timestamp on new posts, like 10m ago, or an absolute timestamp, like January 7, 2020 at 12:15PM. Comments and replies are also shown with relative timestamps.

1. In Setup, enter *Chatter* in the Quick Find box and select *Chatter Settings*.

2. To show relative timestamps on new posts, comments, and replies in case feeds, select **Show relative timestamps**. To show absolute timestamps, deselect the setting.

    When **Show relative timestamps** is selected, case feed posts less than two days old show relative timestamps. After two days, timestamps on case feed posts change to absolute. Case feed comment timestamps remain relative. When relative timestamps are shown, users can see the absolute timestamp by hovering over the stamp.

EDITIONS

Available in: Lightning Experience

Available in: **Essentials**, **Group**, **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Contact Manager** editions.

USER PERMISSIONS

To set up case feed timestamp format:
- Customize Application

Convert Character Combinations into Emoticons in the Feed

Emoticons let your users enter character combinations in their posts and comments to create expressions.

Emoticons are supported in Lightning Experience, Salesforce Classic, and the Salesforce app.

1. From Setup, enter *Chatter Settings* in the Quick Find box, then select **Chatter Settings**.

2. In the Emoticons in Feed section, select **Allow Emoticons**.

Salesforce supports these character combinations in posts and comments.

EDITIONS

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

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

USER PERMISSIONS

To enable emoticons:
- Customize Application

Character Combinations	Emoticon
- :) - :-)	😊 (smile)
- :P - :-P - :p - :-p	😛 (tongue)
- :(- :-(	😦 (frown)
- >:(- >:-(	😠 (angry)
- :((	😢 (crying)

Character Combinations	Emoticon
• :'(	
• :'-(	

Let Users Set Out-of-Office Messages in Chatter

Let your users schedule and customize an out-of-office message, and place it next to their name in Chatter. You can enable or disable this feature in Setup, under Chatter Settings. Setting an out-of-office message is available only in Lightning Experience.

1. In Setup, go to **Chatter Settings**.

2. Click **Edit**.

3. In the **Out of Office** section, enable (or disable) **Users can set Out of Office messages**.

4. Click **Save**.

Customer Invitations

Let users invite customers to the private groups that they own or manage. Customers are users outside of your company's email domains. They have limited Chatter access and can see only the groups that they're invited to. They can interact only with members of those groups.

Customer invitations don't support My Domain URLs or domains created with single sign-on or IP restrictions. To enable customer invitations with these features in place, we recommend one of the following approaches:

- Customize the single sign-on page for your organization with an extra link redirecting users to `https://MyDomainName.my.salesforce.com/`.
- Enable single sign-on for your customers.

Customer invitations are enabled by default. To disable customer invitations, go to Setup and enter `Chatter` in the `Quick Find` box. Select `Chatter Settings`, and deselect `Allow`

`Customer Invitations` in the Chatter Settings section. Disabling customer invitations doesn't delete existing customers or groups that allow customers.

SEE ALSO:

[Coworker Invitations](#)

Coworker Invitations

Let Salesforce users invite coworkers without Salesforce licenses to Chatter. Invited users can access Chatter people, profiles, groups, and files, but they can't see record data unless they have a Salesforce license.

Coworker invitations are automatically enabled for new Salesforce organizations. The email domain of the first Salesforce user who is added to the organization is used as the company domain in the **Company Email Domains** field. Coworker invitations aren't enabled if the first Salesforce user's domain is a free public email provider such as yahoo.com or gmail.com.

In the **Company Email Domains** field, enter the domains that are used in your company's email addresses. You can enter up to 200 domains. Avoid public email domains such as hotmail.com, yahoo.com, or gmail.com. If invited, anyone with an email address in these domains can join and see user profiles, feeds, and Chatter groups.

To disable coworker invitations, go to Setup and enter `Chatter` in the `Quick Find` box. Select `Chatter Settings`, and deselect `Allow Coworker Invitations` in the Coworker Invitations section. If you deselect this feature, users can't accept outstanding invitations. Similarly, if you remove an email domain, users can't accept outstanding invitations from that domain.

SEE ALSO:

[Customer Invitations](#)

EDITIONS

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

Salesforce CRM, Approvals, Chatter email notifications, Chatter Invitations, and customer invitations are not available in **Database.com**.

Enable Add Actions in the Chatter Publisher

In Salesforce Classic, before you can add global actions to the Chatter publisher, you must first enable the Actions in the Publisher feature in Chatter Settings. Actions add functionality to the Chatter publisher and let your users do more in Salesforce across every device.

1. From Setup, enter `Chatter Settings` in the `Quick Find` box, then select **Chatter Settings**.

2. Click **Edit**.

3. In the Actions in the Publisher section, select **Enable actions in the publisher**.

4. Save your changes.

SEE ALSO:

[Publisher Actions and Layouts](#)

EDITIONS

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

USER PERMISSIONS

To enable actions:
- Customize Application

Feed Post and Comments Editing Overview

With feed post editing, users can edit their own feed posts. Record owners can also edit any post on records they own, no matter who created the post.

A Chatter Settings option and user permissions control the availability of the feed post editing feature.

> **Note:** In addition to permissions, sharing rules can affect user access to feed post editing, including who can delete a post.

The `Allow users to edit posts and comments` option in Chatter Settings enables or disables the Edit Feed Post feature for your organization. This option is enabled by default in existing and new organizations. All users who are assigned a standard profile can edit their own posts and comments immediately, except for Chatter Free, Chatter External, and Customer Portal users. For users who are assigned custom profiles, administrators must specifically enable the permissions in the users' custom profiles or permission sets.

The "Edit My Own Posts" permission lets users edit their own posts. This permission is available and automatically enabled on standard profiles, except Chatter External, Chatter Free, and Customer Portal User profiles. To allow Chatter External, Chatter Free, or Custom Portal users to edit their own posts, clone the profiles. Enable the "Edit My Own Posts" permission in the cloned profiles. Then assign the cloned profiles to the users.

The "Edit Posts on Records I Own" permission lets users edit all posts and comments on the records they own—both their own and other users'. For example, a group owner or manager can edit all posts on the group's feed. A manager for a particular record type can edit all posts on the record. This permission is available on standard and custom profiles, but it's disabled by default.

The "Can Approve Feed Post and Comment" permission is a powerful option to consider when assigning editorial capability. Users with this permission can edit and delete the posts and comments of any person in the Chatter feeds that they have access to. Consider whether it's useful to have a few users with this capability. But also consider that assigning this permission places whoever has it in a position of trust. Be thoughtful about whom you assign it to.

This table summarizes the permissions and their default settings.

User Permission	Description	Available in	Default Setting
Edit My Own Posts	Allows users to edit their own posts	Standard profiles, except • Chatter External User • Chatter Free User • High Volume Customer Portal User • Partner Community User Profile	Enabled in all new and existing organizations
		Custom profiles	Disabled in all new and existing organizations
Edit Posts on Records I Own	Allows record owners to modify their own posts and posts other users made on groups and record detail pages.	Custom profiles	Disabled in all new and existing organizations. However, Chatter moderators, Experience Cloud site moderators, and users with "Modify All Data" permission can always edit all posts and comments.

The `Allow users to edit posts and comments` option in Chatter Settings is enabled by default. For users who have the required permissions, the Edit option is available from the menu on posts, comments, questions, and answers. It opens a separate Edit window, where users can modify the text.
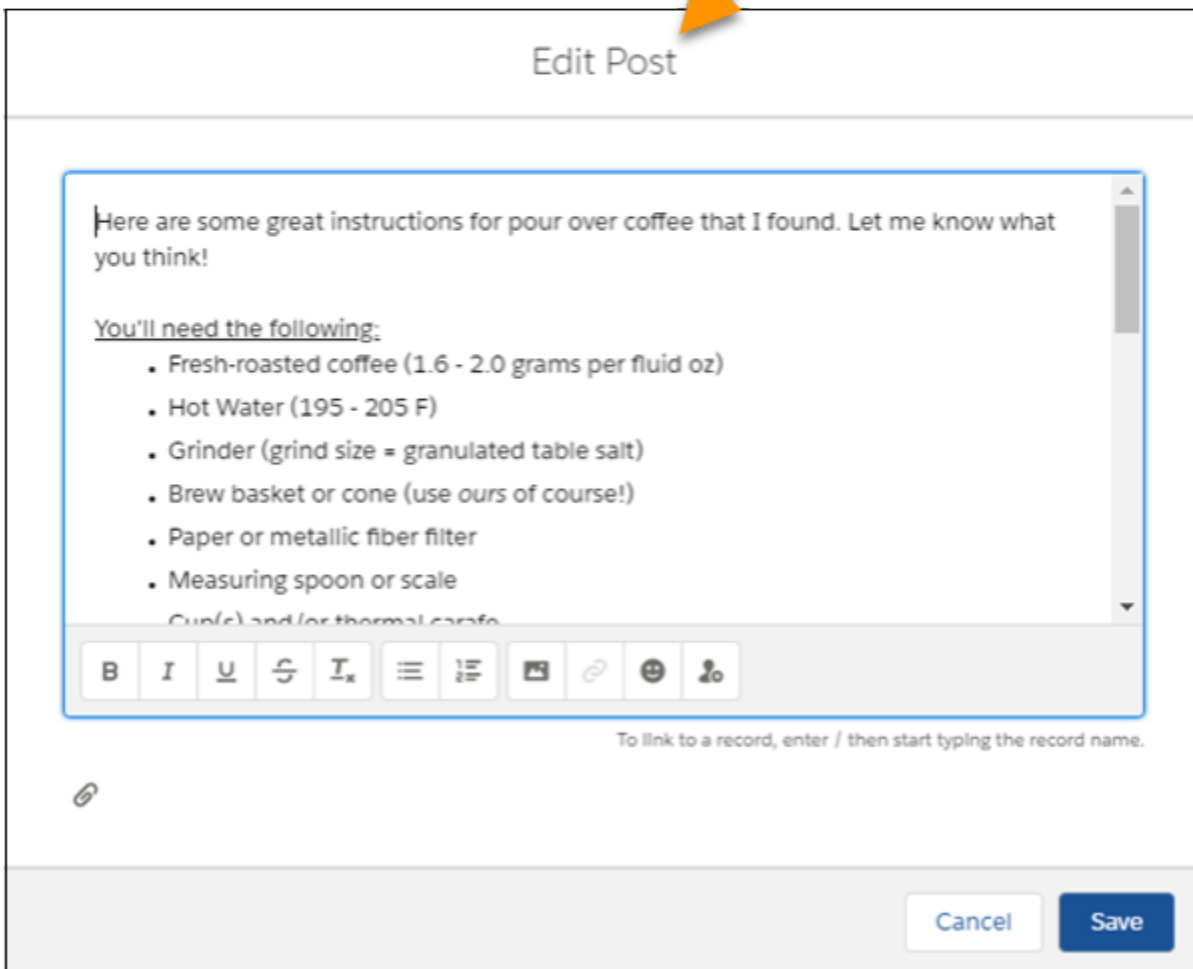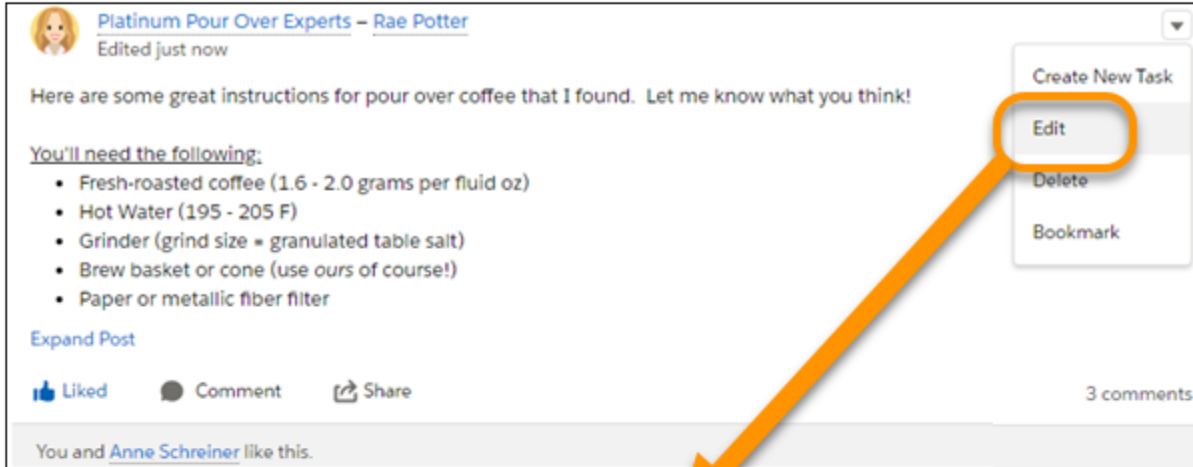
After users save their edited version of the post, it shows an Edited timestamp to indicate that the original post was modified.
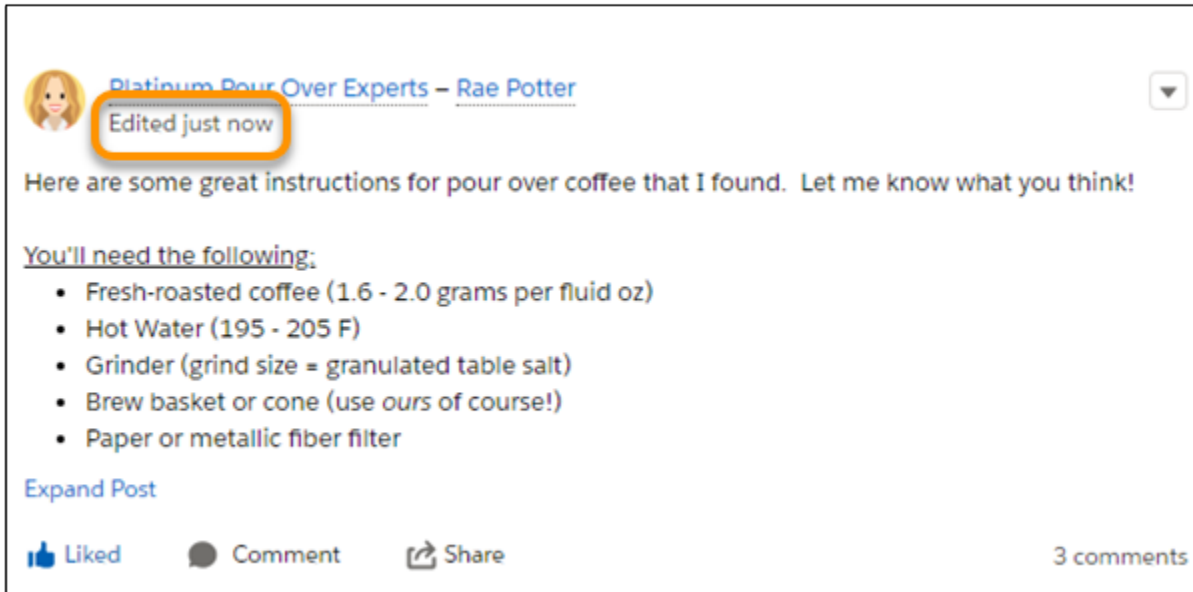
If users edit a post or comment and mention new people or groups, those people and groups receive email notifications. But the people and groups who were mentioned in the original post or comment don't receive a new email notification. Email notifications for edited posts or comments show the Edited timestamp.

For Experience Cloud site users, feed post editing is available only if the site was created using either Salesforce Tabs + Visualforce or the Customer Service template.

The Edit option isn't available on system-generated posts like feed tracked record updates.

Enable Edit Feed Post in User Profiles or Permission Sets

By default, feed post editing is disabled on all custom profiles. To make the feature available to your users, you can either modify your user profiles or assign the permissions to users via a permission set.

Disable Edit Feed Post for All Users

By default, all users who are assigned a profile with the feed post editing permissions enabled can edit their posts and comments. If needed, you can disable feed post editing for all users in your organization, regardless of their assigned user profile. You can also shut off post and comment editing for all users assigned the "Can Approve Feed Post and Comment" permission.

Enable Edit Feed Post in User Profiles or Permission Sets

By default, feed post editing is disabled on all custom profiles. To make the feature available to your users, you can either modify your user profiles or assign the permissions to users via a permission set.

Here's how you enable the permissions in a permission set.

1. From Setup, enter `Permission Sets` in the `Quick Find` box, then select **Permission Sets**.

2. Click an existing permission set or create one.

3. Click System Permissions, and then click **Edit**.

4. Select the edit feed post permissions you want to enable.

USER PERMISSIONS

To create custom profiles
- Manage Profiles and Permission Sets

To assign permission sets
- Assign Permission Sets

- *Edit My Own Posts*—Let users edit their own posts and comments.
- *Edit Posts on Records I Own*—Let users edit posts and comments on records they own. This setting applies to all posts and comments on a record, both by the author and made by other users.
- *Can Approve Feed Post and Comment*—Let users edit and delete the posts and comments of any person in the Chatter feeds that they have access to.

5. Click **Save**.

6. Assign the permission set to the users who need the permissions.

Disable Edit Feed Post for All Users

By default, all users who are assigned a profile with the feed post editing permissions enabled can edit their posts and comments. If needed, you can disable feed post editing for all users in your organization, regardless of their assigned user profile. You can also shut off post and comment editing for all users assigned the "Can Approve Feed Post and Comment" permission.

1. From Setup, enter *Chatter Settings* in the *Quick Find* box, then select **Chatter Settings**.

2. Click **Edit**.

3. In the Post and Comment Modification section, deselect the checkbox on *Allow users to edit posts and comments*.

> **Post and Comment Modification**
>
> The author of the post or comment, the record owner, a Chatter moderator, and a moderator in this community have permission to modify the text.
>
> Allow users to edit posts and comments ☐

4. Click **Save**.

5. If you have assigned the "Can Approve Feed Post and Comment" permission, disable that on the relevant permission sets.

    "Can Approve Feed Post and Comment" lets assigned users edit and delete any post or comment in any Chatter feed those users have access to. This permission is available under **Setup** > **Permission Sets** > *Select a permission set* > **System Permissions**.

The feed post editing feature is disabled for your entire organization (or, for step 5, for all users assigned the edited permission set). Users can no longer edit posts and comments.

Publisher Actions and Layouts

Actions add functionality to the Chatter Publisher in Salesforce Classic. Actions let your users do more in Salesforce across all devices.

Actions are all about productivity. Actions let users accomplish things with fewer clicks, fewer fields, and ultimately less time spent. Actions are especially useful in the Salesforce app, because it makes it easy to create and edit records with a simple, mobile-optimized interface. By default, the Chatter publisher includes the standard actions Post, File, Link, Poll, and Question.
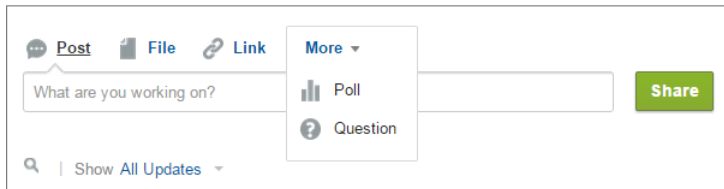
Actions appear in the action bar, its associated action menu, and as list-item actions.
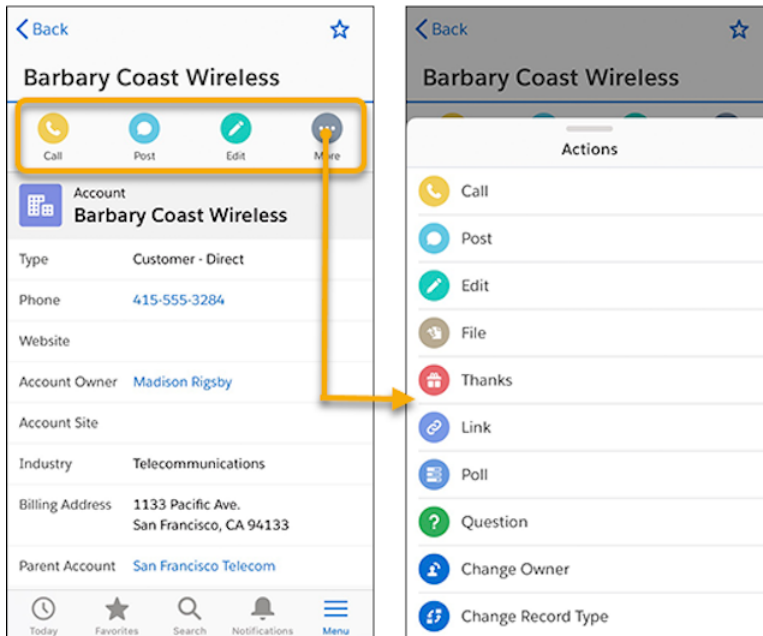
There are several categories of actions, like standard actions, nonstandard actions, default actions, mobile smart actions, custom actions, and productivity actions.

- **Standard actions**: Standard actions are actions that are automatically added to the publisher when Chatter is enabled—such as Post, File, Link, and Poll. You can customize the order in which these actions appear in the publisher, but you can't edit their properties.
- **Nonstandard actions**: Nonstandard actions are actions that you create and customize yourself.
- **Default actions**: Default actions are predefined actions provided by Salesforce. To make them available to your users, add them to the Chatter publisher layout.
- **Mobile smart actions**: Mobile smart actions are a set of preconfigured actions, just like default actions. Mobile smart actions let users create records directly in the feed.
- **Custom actions**: Custom actions are Visualforce pages or canvas apps with functionality that you define. For example, you can create a custom action so that users can write comments that are longer than 5000 characters.
- **Productivity actions**: Salesforce predefines productivity actions. They are attached to account, contact, event, lead, user, and user profile objects. You can't edit or delete productivity actions.

To customize the publisher with actions or change the order of actions, first enable actions in the publisher. Enable actions in Setup on the Chatter Settings page.

Enable Code Snippets and Assign Permissions to Use Them

Use code snippets to enter syntax-highlighted code samples through the Chatter publisher. To make code snippets available, enable them and assign the permission to use them. There are two ways to enable code snippets and assign permission: through a user profile (step 1) or through a permission set (step 2). Code snippets are available in Lightning Experience and Experience Builder sites that are based on the Customer Service template.

1. Enable code snippets through a user profile:

    a. In Setup, expand **Manage Users** (**Users** in Lightning Experience), click **Profiles**, then click **Clone** next to **Standard User**.

    b. Give the clone a **Profile Name**, and click **Save**.

    c. On the clone page, click **Edit**.

    d. Scroll to the **General User Permissions** section, select **Allow Inclusion of Code Snippets from UI**, and click **Save**.

    e. Under **Manage Users**, click **Users**.

    f. Edit each user you want to give code snippet permission to, and assign them the cloned user profile.

2. Enable code snippets through a permission set:

    a. In Setup, expand **Manage Users** (**Users** in Lightning Experience), click **Permission Sets**, then click **New**.

    b. In the **Label** field, enter a name for the permission set.

    c. Optionally, pick a type of user license for this permission set. Pick **None** if you don't want to limit this permission set to a particular license type.

    d. Click **Save**.

    e. On the new permission set page, under **System**, click **System Permissions**, then click **Edit**.

    f. Select **Allow Inclusion of Code Snippets from UI**, and click **Save**.

    g. Click **Manage Assignments**, then **Add Assignments**.

    h. Assign the new permission set, then click **Done**.

Your users can enter code snippets in the Chatter publisher. Users can't add a code snippet to a list.

Assign Pin Post Permission

Pin your most critical information to the top of a feed. In group and topics feeds, an authorized user can pin up to three posts. A pinned post stays in place until an authorized user unpins it. After you enable post pinning through Chatter Settings, you can assign the Pin Posts in Feeds permission through a permission set or a user profile.
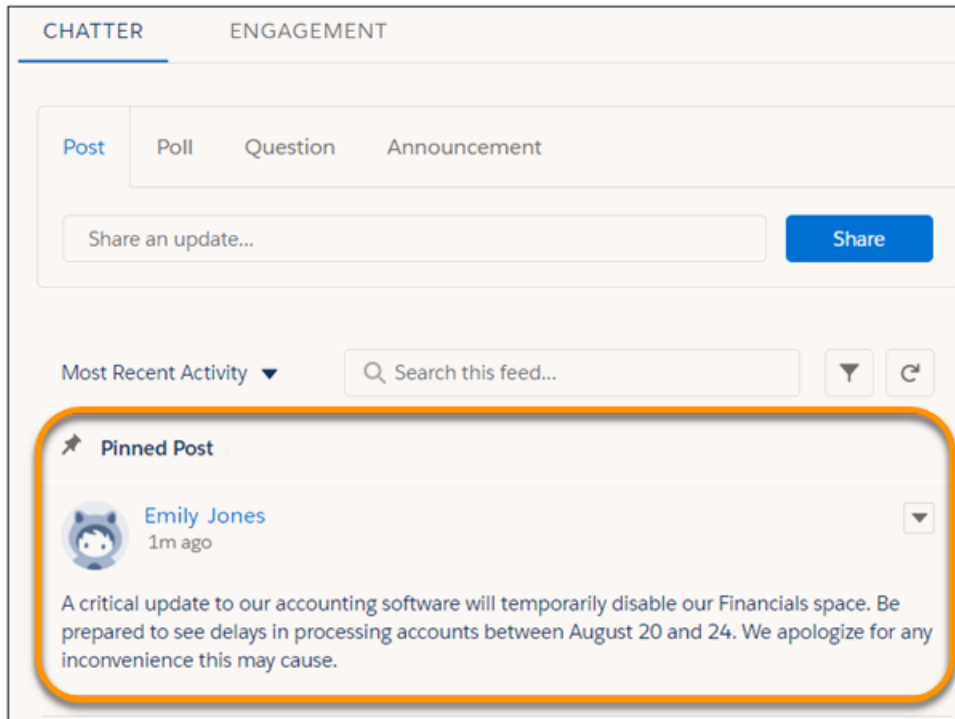
EDITIONS

Available in Lightning Experience in: **Essentials**, **Group**, **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Contact Manager** Editions

USER PERMISSIONS

To assign post pinning permission to a user:
- Enable Chatter

When all permissions are in place, the **Pin** option appears on a feed item's overflow menu in group and topics feeds. The **Pin** option isn't available in the feed item's detail view.

Start by enabling post pinning for your org. Go to **Setup** > **Chatter Settings**, and select **Allow post pinning**. After post pinning is enabled, admins, group owners, and group managers can pin posts. Admins can also assign the Pin Posts in Feeds permission to users through user profiles or permission sets.

When you pin a post, it appears twice in the feed: where it was posted and in its pinned position at the top of the feed. You can pin only the posts that were added directly to the feed. You can't pin posts that were added through an @mention.

Pinned posts are similar to announcements, with these differences.

- Announcements are available only to group feeds. Post pinning is available to group and topics feeds.
- Announcements follow a linear timeline: you post it and you let it expire. Pinned posts are more flexible: you can pin posts from the past or the present.
- An announcement expires on a set date. A pinned post stays pinned until an authorized user unpins it.
- Only group owners and managers and users with the Modify All Data permission can post and delete group announcements. Admins can choose who is authorized to pin posts.
- You can post only one announcement per group feed. Authorized users can pin up to three posts to the top of a feed.
- You can add style to a pinned post with the rich text editor.

SEE ALSO:

Pin Posts in an Experience Cloud Site

Feed Tracking

Feed tracking detects changes to tracked record fields and posts them as updates in the What I Follow feed. Users who follow a record, see those updates in their view of What I Follow, with one exception. Updates users make themselves aren't posted to What I Follow. Users can see those updates in their profile feeds.

Feed tracking is available for record fields. You can configure feed tracking for users, Chatter groups, topics, custom objects, external objects, and the following standard objects: accounts, article types, assets, campaigns, cases, contacts, contracts, dashboards, events, leads, opportunities, products, reports, solutions, and tasks.

> 📝 **Note:** In Lightning Experience, most object records don't show a Chatter tab unless Feed Tracking is enabled for the object. Exceptions include Group, Site, and User objects.

Sharing rules and field-level security determine the visibility of record changes in Chatter feeds. To see changes to a record in their feeds, users must have access to the record.

These objects and fields are tracked by default:

- Account: `Account Name, Account Owner`
- Case: `Case Owner, Priority, Status`
- Chatter Group: `Allow Customers, Description, Group Access, Information Body, Information Title, Name, Owner Name`
- Contact: `Account Name, Contact Owner, Name`
- Lead: `Lead Owner, Lead Status, Name`
- Opportunity: `Amount, Close Date, Opportunity Name, Opportunity Owner, Stage`
- Topic: `Description`
- User: `About Me, Address, Email, Manager, Phone, Title`

Tracked feed updates that are older than 45 days and have no likes or comments are deleted automatically. The tracked feed updates no longer appear in the feed. However, if auditing is enabled for a tracked field, the tracking field audit history is still available.

> 📝 **Note:** Reports on feed activities don't include information about system-generated posts, such as feed tracked changes.

Tracked changes in a feed can be bundled together for quick and easy reading. This image shows two tracked change notifications bundled together. On this record, Bat Chad changed the values for the Product Owner and QA Engineer fields.

Customize Chatter Feed Tracking

When you enable feed tracking for objects and records, users see updates for the objects and records that they follow in their What I Follow feed. Many objects and fields are tracked by default, but you can further customize feed tracking to include or exclude specific objects and fields.

Feed Tracking Limitations

Here are some limitations on tracking objects, fields, and topics.

Feed Tracked Change Bundles

We save you time and space in your feeds by bundling multiple feed tracked change updates into a quick-reference list. Bundles are collections of feed tracked change items that you see in feeds. You can see bundles in your browser. In Salesforce for Android and Salesforce for iOS, bundles appear only in record feeds.

SEE ALSO:

Chatter Settings

Feed Tracked Change Bundles

Customize Chatter Feed Tracking

When you enable feed tracking for objects and records, users see updates for the objects and records that they follow in their What I Follow feed. Many objects and fields are tracked by default, but you can further customize feed tracking to include or exclude specific objects and fields.

You can configure feed tracking for users, Chatter groups, topics, custom objects, and external objects. You can also set up feed tracking for the following standard objects:

- accounts
- article types
- assets
- campaigns
- cases
- contacts
- contracts
- dashboards
- events
- leads
- opportunities
- products
- reports
- solutions
- tasks

📝 **Note:** In Lightning Experience, most objects don't show a Chatter tab unless feed tracking is enabled for the object. The only exceptions are Group, Site, and User objects. The What I Follow feed shows updates to the tracked fields on the people and objects that a user follows. There's one exception. Updates that report a user's own changes to a tracked field appear in the user's profile feed, but not in What I Follow.

1. From Setup, enter `Feed Tracking` in the `Quick Find` box, then select **Feed Tracking**.
2. Select an object.
3. Select `Enable Feed Tracking`.

   You must have the required user permissions to see the Enable Feed Tracking checkbox.

4. Select up to 20 of the object's fields to track.

   You can't select fields for external objects or article types. These standard field types can't be tracked:

   - Auto-number, formula, and roll-up summary fields
   - Encrypted and read-only system fields
   - The `Expected Revenue` field on opportunities
   - The `Solution Title` and `Solution Details` fields on solutions. These fields appear only for translated solutions in organizations with multilingual solutions enabled

5. If you have actions in the publisher enabled, you see the `All Related Objects` option. To show feed items when related objects are created, select this checkbox.

> **Note:** To enable actions in the publisher, in the Setup Quick Find box, enter `Chatter`, and select Chatter Settings. Under Actions in the Publisher, select Enable Actions in the Publisher.

6. Save your changes.
When a value in a tracked field changes, users see a notification about the change in the appropriate feed.

SEE ALSO:

Feed Tracking

Feed Tracking Limitations

Here are some limitations on tracking objects, fields, and topics.

- Reports on feed activities don't include information about system-generated posts, such as feed tracked changes.
- When feed tracking is enabled for person accounts, users can follow and see updates to account fields, but not to contact fields.
- Feed tracking for events doesn't include requested meetings. Once a requested meeting is confirmed and becomes an event, then it can be tracked.
- User can follow activities and knowledge articles in a Chatter feed. However, the ⊕ **Follow** button in the Action column for activity and knowledge article list views isn't available.
- If you disable feed tracking for topics, users cannot follow new topics. They can continue to follow the topics they followed when feed tracking was enabled. The followed topics count toward the maximum number of things they can follow. Use the Connect REST API to stop following topics after feed tracking is disabled.
- Most feed tracking changes are reported in the What I Follow feed. However, users' own changes to tracked fields are reported in their profile feeds instead.

Feed Tracking Limitations on External Objects

- Field history tracking isn't available for external objects.
- Record feeds aren't available for Salesforce Connect external objects that map to high-data-volume external data sources.

Feed Tracked Change Bundles

We save you time and space in your feeds by bundling multiple feed tracked change updates into a quick-reference list. Bundles are collections of feed tracked change items that you see in feeds. You can see bundles in your browser. In Salesforce for Android and Salesforce for iOS, bundles appear only in record feeds.

EDITIONS

Available in: **Essentials**, **Group**, **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Contact Manager**, and **Developer** Editions
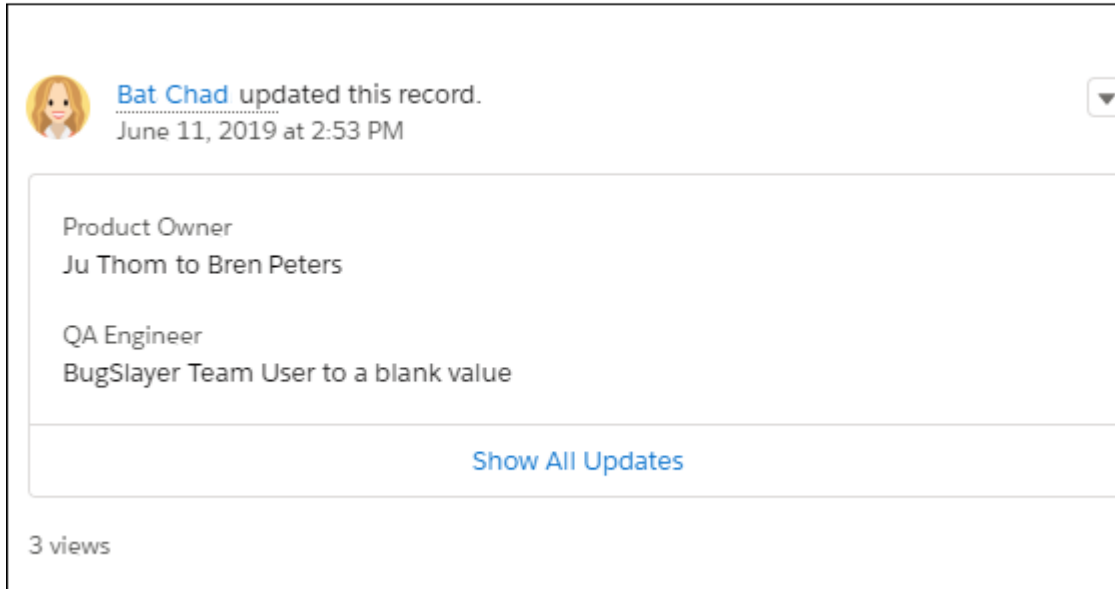
Feed tracked changes (FTCs) are bundled when at least three FTCs with the same parent ID are formed within a specified time. The default time is 1,440 minutes. New FTCs are added to the same bundle, as long as the interval of the bundle is within a specified time. The interval measurement comes from comparing the created date of the oldest FTC to the newest. The default interval is 10,080 minutes.

📝 **Note:** If you want to change the default time or interval, contact Salesforce Customer Support.

When someone comments on a bundled FTC, it's removed from the bundle and placed on its own in the feed. FTCs without comments or likes are deleted and removed from the bundle after 45 days. If the number of FTCs in an existing bundle drops to two, the bundle's nonetheless preserved. If the number of FTCs in a bundle drops to one, the bundle's deleted, and the single FTC appears on its own in the feed.

📝 **Note:** Tracked feed updates that are older than 45 days and have no likes or comments are deleted automatically. The tracked feed updates no longer appear in the feed. However, if auditing is enabled for a tracked field, the tracking field audit history is still available.

Chatter Email Settings and Branding

Chatter email settings let you change the format of your company's outgoing emails and control whether users receive email notifications.

If Chatter is enabled, email notifications are enabled by default. However, your users can configure their own email settings. They control whether they want to receive emails, how often they receive them, and the types of changes that trigger notifications. It's important that your users know how to control the amount of email they receive. Too many email notifications are a pain point for many Chatter users and a common barrier to adoption.

Configure general Chatter email settings and branding from Setup. Enter `Email Settings` in the `Quick Find` box, then select **Email Settings**. This table describes the settings.

Setting	Description
General Settings	

Setting	Description
Allow Emails	Enables or disables email notifications for your entire company. If you deselect this option, all email notifications are disabled and your users don't receive notifications.
Allow Email Replies	If selected, users can reply to email notifications about messages and comments via email instead of navigating to the comment or message in Chatter.
Allow Posts via Email	If selected, users can post to groups through email.
Allow Attachments via Email	If selected, users can include attachments on posts to groups that are made through email.
Show mobile app download badges	Show App Store and Google Play download badges for Salesforce in all Chatter email notifications from your internal org. Badges don't appear in email notifications from Experience Cloud sites. A recipient's language setting affects whether badges appear: if a badge isn't translated in the set language, it doesn't appear in the email. The show badges option is selected by default.
Allow API-only Chatter Digests	This setting appears only if API-only Chatter Digests are enabled for your company. To enable this feature, contact Salesforce. When you select this option, daily and weekly scheduled digests are disabled for your entire company. To provide digests to your users, you must call the API.
Sender	
From Name	The name that appears as the sender's name in the email notification. Enter a name in this field if you want the sender name to contain a static value, such as your company's name. If you leave this field blank, a dynamic name is used.
Email Address	The email address of the sender. For example, add your company's email address. This field is required for Chatter email notifications to be sent. A few things to keep in mind: • If the `Allow Email Replies` setting isn't selected, then replies sent via email go directly to this email address and don't appear on the Chatter post. • Chatter email notifications are only sent from verified email addresses. • Don't use a distribution email list in this field. Verification emails are sent when this field is populated. If you use a distribution email list, verification emails are sent to everyone in that list.
Branding	

Setting	Description
Logo	The Chatter logo appears in the email notification by default. To keep your email notifications consistent with your company's brand, upload your company logo and replace the default.
Footer Text	The text that appears in the footer of the notification email. We strongly recommend including your company's physical address to comply with applicable anti-spam laws.

[Add Your Custom Brand to Email Notifications](#)

Customize your company's Chatter email notifications to show your company's sender information, footer text, and footer logo.

Add Your Custom Brand to Email Notifications

Customize your company's Chatter email notifications to show your company's sender information, footer text, and footer logo.

1. From Setup, enter `Email Settings` in the `Quick Find` box, then select **Email Settings**.

2. Enter custom values for the email sender's name and address to replace the default values.

   📝 Note: If you change the sender's email address, we send a verification email to the new address. The change is pending, and we continue to use the existing address while we await verification. The requested address doesn't take effect until you click the confirmation link in the email. If verification is already pending for a new email address, and you specify a different new address, we retain the latest value and use that value for verification.

   If you enter a custom value for the sender's address and you have enabled mail relay, your Chatter emails use the relay.

3. Customize what displays in the footer of Chatter emails.

   📝 Note:
   - All Chatter emails display the Chatter logo and Salesforce information unless you replace them with your organization's own logo and information.
   - If you previously customized the logo or footer text and want to restore the default values, use the API to set these fields to `null`.

   a. To replace the default Chatter logo, choose a logo.

      The logo must be an existing document in the Documents tab and must be marked Externally Available Image. Images of 150 x 50 pixels on a transparent background work best.

   b. To replace the default footer text, enter up to 1,000 characters.

      The default text includes the Salesforce name and physical address. We recommend including your org's physical address to comply with applicable anti-spam laws.

4. Click **Save**.

SEE ALSO:

[Chatter Email Settings and Branding](#)

Chatter Post Actions and Layouts

Actions on posts and comments appear in the drop-down menu on a post or comment. Users can edit, bookmark, mute, and delete posts, add topics, and create tasks from posts.

The standard Bookmark, Delete, Mute, and Add Topic actions on posts are available by default and you can't modify them. However, you can add more actions like the Edit and Create New Task actions.

Enable Create New Tasks on Posts
Enhance the feed with an action that lets users create tasks directly from a post.

Enable Create New Tasks on Posts

Enhance the feed with an action that lets users create tasks directly from a post.

Actions in the Publisher and feed tracking for the Task object must be enabled.

1. From Setup, enter `Feed Item` in the `Quick Find` box, then select **Feed Item Layouts**.

2. Click **Edit** next to Feed Item Layout.

3. In the Feed Item Layout, click **Quick Actions**.

4. For Salesforce Classic, select the **Create New Task** action and drag it to the Actions in the Publisher section.
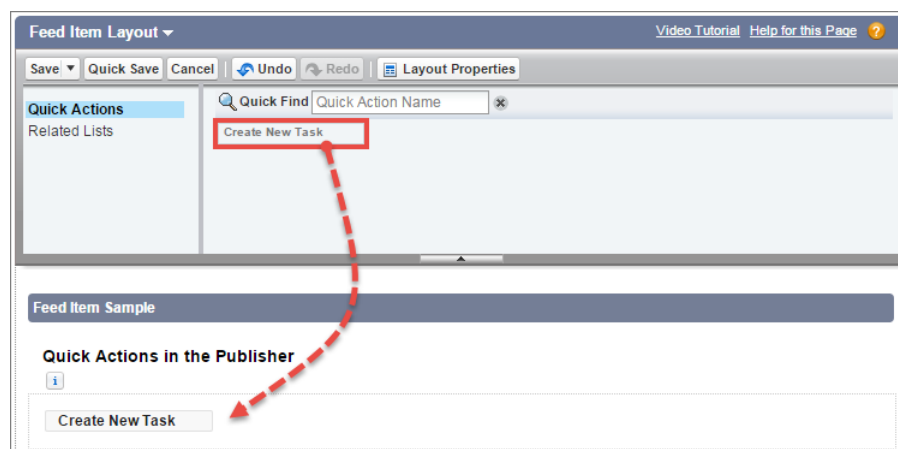
For Lightning Experience, drag **Create New Task** to the Salesforce Mobile and Lightning Experience Actions section.

If you don't see the Create New Task action, verify that the Actions in the Publisher feature is enabled under Chatter Settings in Setup.

5. Save your changes.

The Create New Task action displays on a post's menu. When a user creates a task from a post, the task shows up in the My Task list on the user's Home page. The Create New Task action on posts

• Is available on user-entered posts, but not on system-generated posts like tracked feed updates

• Can be partly customized. You can't change the fields, but you can change the layout of the fields.

• Generates an update that appears in the user's feed

Group Layouts

The group layout lets you customize which fields, buttons, actions, and lists appear in Chatter groups. Changes to the group layout affect all groups in your organization, but they appear only on the group pages in the Salesforce mobile app. Changes to the group publisher appear in both the full Salesforce site and the Salesforce mobile app.

The changes you make to the group layout and the publisher affect all groups in your organization. You can't customize the layout of an individual group.

Customize the Chatter Group Layout and Publisher
Add and remove fields, buttons, look-ups, and related lists to change the layout of groups.

Add Actions to the Group Publisher
Customize the group publisher with quick actions and Salesforce mobile app actions.

Customize the Chatter Group Layout and Publisher

Add and remove fields, buttons, look-ups, and related lists to change the layout of groups.

1. From Setup, enter `Group Layouts` in the `Quick Find` box, then select **Group Layouts**.

2. Click **Edit** next to the group layout that you want to customize, or click **New** to create a layout.

3. From the palette on the top of the page, drag fields, buttons, and other user interface elements. Drag these elements to different sections to add them to the group layout. To remove elements from the layout, drag them back to the palette. To make sure your action works in the Salesforce mobile app and Lightning Experience, be sure the following are in your group layout:

   - Post
   - Announcement (announcements aren't available in the Salesforce mobile app)
   - File
   - Poll
   - Edit Group
   - New Group Member
   - Manage Notifications
   - Delete Group
   - Leave Group

All group layout changes affect the Salesforce mobile app and Lightning Experience. Group publisher changes appear everywhere. For example, imagine that you delete the Files related list or a field in the Group Details section. Your changes appear only in the app and Lightning Experience. They don't appear in Salesforce Classic.

4. To save the layout, click **Save**.

👁 **Example:** Let's allow group owners and managers to archive and activate groups from the Salesforce mobile app and Lightning Experience. Drag the Archive field to the Group Detail section.

To assign group layouts by user profiles, click **Page Layout Assignment** on the group layout list view.

Add Actions to the Group Publisher

Customize the group publisher with quick actions and Salesforce mobile app actions.

By default, Chatter groups offer standard actions that are part of the global publisher layout, like Post, File, Link, and Poll. Override the global publisher layout with a customized group publisher layout.

1. From Setup, enter `Groups` in the `Quick Find` box, then select `Group Layouts`.

2. Click **Edit** next to the group layout that you want to customize, or click **New** to create a layout.

3. Click **override the global publisher layout** in the Quick Actions in the Salesforce Classic Publisher section or **override the predefined actions** in the Salesforce Mobile and Lightning Experience Actions section.

   Changes to the Quick Actions in the Salesforce Classic Publisher section appear in the full Salesforce site. Changes to the Salesforce Mobile and Lightning Experience Actions section appear in the Salesforce mobile app and Lightning Experience. In groups that allow customers, the publisher shows only standard actions.

4. Drag actions between the palette and the publisher layout to add, remove, and reorder actions.

5. Click **Save**.

👁 Example: Add the Announcement and Add Record actions to the group publisher.

EDITIONS

Available in: **Essentials**, **Group**, **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Contact Manager**, and **Developer** Editions
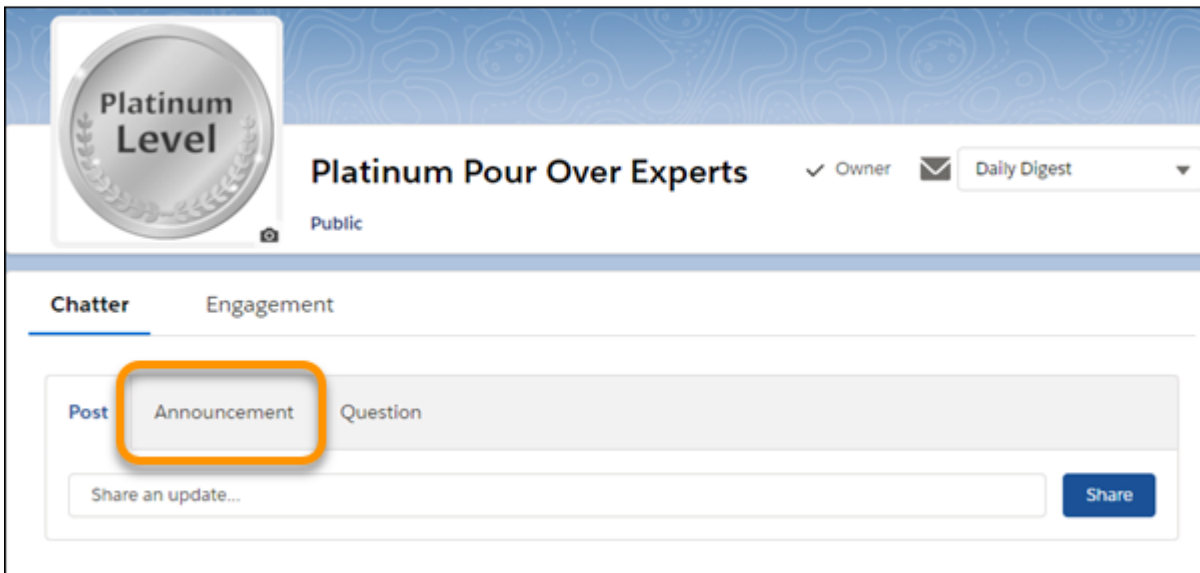
USER PERMISSIONS

To customize Chatter group layouts:
- Customize Application
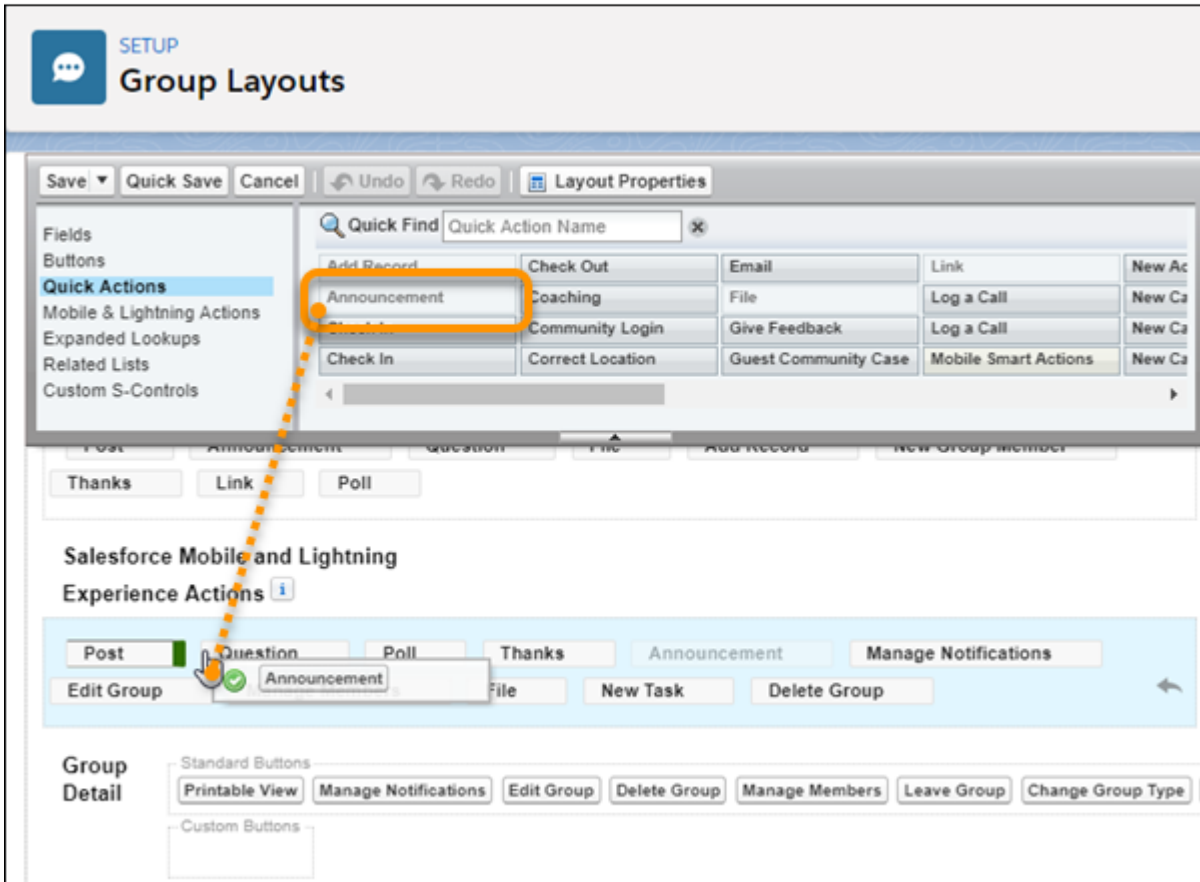
Now users can select this action directly in the publisher.

Topics for Objects

Topics for objects offers a powerful way to crowdsource your company's key themes and issues. Users can add topics to records to organize them by common themes.

Your employees can add topics to records based on what they're seeing in the field and from working with customers. In this way, topics can give your business insight into the voice of your customer. And because topics can cross objects, they can provide connections across people, conversations, and records.

If your company uses Chatter, users can also add topics to posts. Topics on posts help users organize posts and increase their visibility. Topics are great for discussing a particular issue, theme, or subject, that isn't limited to a particular group of people. For example, imagine that your company has created a year-long goal around volunteering with local schools. You can create a topic to allow your entire company to share posts, photos, and updates related to the company goal.

Users can search Chatter posts and Knowledge articles by topic. No other tagged record types return search results.

Configure Topics for Records in Lightning Experience

Add the Topics component to record pages so that your users can assign topics to records. Topics allow your users to organize records by theme. On the topic detail page, users can see all the records with a topic and filter their record list views by topic.

Enable and Configure Topics for Objects in Salesforce Classic

Enable topics for objects so that users can add topics to records and organize them by common themes. This powerful feature is available with or without Chatter.

Delete Topics

People with the right permissions can delete topics directly from topic detail pages.

Topics Privacy

Topic names and descriptions are not private, even for topics that appear solely in private groups and on records. Posts and records with topics have the same security and privacy as posts and records without topics.
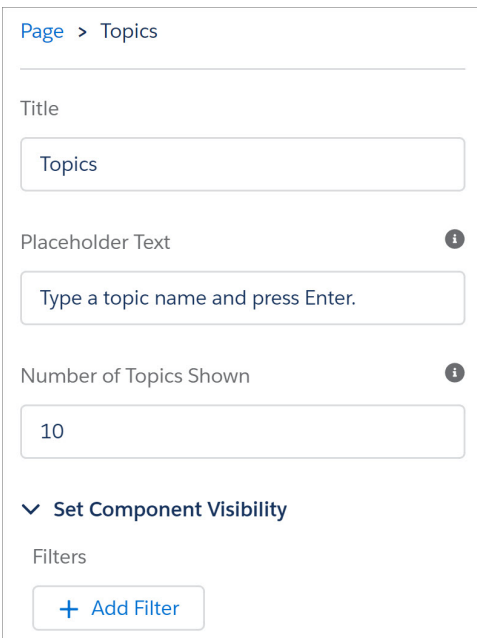
Configure Topics for Records in Lightning Experience

Add the Topics component to record pages so that your users can assign topics to records. Topics allow your users to organize records by theme. On the topic detail page, users can see all the records with a topic and filter their record list views by topic.

By default, topics are enabled for most standard objects. To configure topics for objects, including custom objects, from Setup, enter `Topics for Objects` in the `Quick Find` box, then select **Topics for Objects**.

📝 Note: You can't use encrypted fields for topic suggestions.

1. Create a record page for Lightning Experience.

    If you already have record pages for Lightning Experience, go to the next step.

2. In the Lightning App Builder, configure the Topics component and add it to the page's layout.
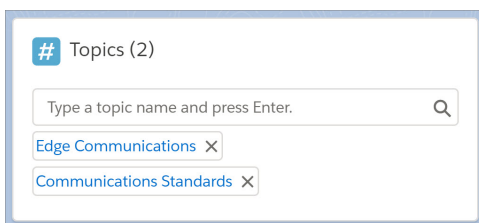
Page > Topics

Title

Topics

Placeholder Text ⓘ

Type a topic name and press Enter.

Number of Topics Shown ⓘ

10

⌄ **Set Component Visibility**

Filters

➕ Add Filter

3. Save your page. If your page is new, activate it.

👁 Example: Users with permission can view, add, and remove topics from records.

\# Topics (2)

Type a topic name and press Enter. 🔍

Edge Communications ✕

Communications Standards ✕

SEE ALSO:

Enable and Configure Topics for Objects in Salesforce Classic

Enable and Configure Topics for Objects in Salesforce Classic

Enable topics for objects so that users can add topics to records and organize them by common themes. This powerful feature is available with or without Chatter.

Available in: Salesforce Classic

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

Administrators can enable topics for accounts, assets, campaigns, cases, contacts, contracts, files, leads, opportunities, orders, solutions, custom objects, and English articles. For each object type, administrators specify which fields to use for topic suggestions.

📝 **Note:** Topics are supported on only English Knowledge articles.

⚠️ **Warning:** When topics are enabled for an object, public tags are disabled for records of that object type.

1. From Setup, enter `Topics for Objects` in the `Quick Find` box, then select **Topics for Objects**.

2. Select an object.

3. At the right, select `Enable Topics`.

4. Select the text fields that you want to use for topic suggestions. (From a combination of the selected fields, up to 3 suggestions are made from the first 2,000 characters.)

   Encrypted fields don't appear in the list of selectable fields because you can't use encrypted fields for topic suggestions.

5. Click **Save**.

Now, users with access to the enabled objects and appropriate topics permissions can:

- See topic assignments and suggestions on records of that object type
- Add and remove topics from records of that object type
- Use topics on records of that object type to filter their list views

If your organization uses Chatter, users can click any topic that is assigned to a record to go directly to a topic page. On a topic page, users see other records on the topic, people who are knowledgeable about the topic, and other related information.

Delete Topics

People with the right permissions can delete topics directly from topic detail pages.

Because topic names and descriptions aren't private, administrators can delete topics for compliance reasons or to remove inappropriate content. When deleting topics, consider these points.

- Topics are permanently deleted. They aren't sent to the Recycle Bin.
- Deleted topics are removed from search results, the topics list, all posts and records, Recently Talked About topics, Related Topics, and your users' favorites. After the next calculation, deleted topics are removed from Trending Topics.
- Users can reintroduce a topic after it's been deleted.

To delete a topic:

1. Navigate to the topic detail page.
2. In the upper right, click **Delete** (Lightning Experience) or [▼] and choose **Delete** (Salesforce Classic).

In Experience Cloud sites, delete topics from **Workspaces** > **Content Management** > **Topics**. After the topics are deleted, they're no longer assigned in your site.

Topics Privacy

Topic names and descriptions are not private, even for topics that appear solely in private groups and on records. Posts and records with topics have the same security and privacy as posts and records without topics.

This table explains where you can see all topics and where you can't see topics that are used solely in private groups or on records.

User interface element	Shows all topics	Doesn't show topics that are used solely in private groups and on records
Topics list	✔	
Topic search results	✔	
Topic reports	✔	
Knowledgeable User reports		✔

User interface element	Shows all topics	Doesn't show topics that are used solely in private groups and on records
Related Topics on the topic detail page	✔	
Recently Talked About topics on group detail pages	✔	
Recently Talked About topics on profiles		✔
Trending Topics on the Chatter page		✔
Topic suggestions when adding topics to a post or a record		✔
People-talking number in the topics list and in topic suggestions when adding topics to a post		✔

For increased security of topic names, Salesforce turns off topics for guest and authenticated external users in Salesforce Sites and in portals created before Summer '13. If you want to enable topics for external users, go to Setup and enter `Chatter` in the Quick Find box. Select Chatter Settings, and in the Topics section select **Allow topics in Salesforce Sites and Portals**.

📝 Note: You can't use topics in unlisted groups. You can add a hashtag topic when you write a post or comment in an unlisted group. The topic is formatted as a link after you post. However, a topic detail page isn't created, and the link doesn't work.

Customize Chatter Influence

Customize activity thresholds for posts, comments, and likes to improve the Chatter influence calculation.

Chatter activity statistics include counts for posts and comments made, comments received, and likes and upvotes on posts and comments.

📝 Note: If upvotes are enabled, they count toward influence as likes received.

1. From Setup, enter `Influence` in the `Quick Find` box, then select **Influence**.

2. Change the minimum activity thresholds.

   All minimum activity thresholds default to zero. If you set higher thresholds, users who don't meet all three minimums are considered observers who aren't counted when calculating influence rank. Users who do meet all three minimums but have relatively low activity are also considered observers, but they're counted when calculating influence.

3. Click **Save**.
   Chatter influence is recalculated when you save these values.

> ⚠️ **Warning:** Use caution when setting new thresholds because users' influence levels can change immediately.

SEE ALSO:

Salesforce Chatter

Allow Users to Thank Their Coworkers

Recognize your coworkers with thanks badges and post your thanks directly to the Chatter feed.

Enabling Chatter Thanks

System administrators must have the "Moderate Chatter" permission for their profile and be using Salesforce Classic to enable Thanks.

1. From Setup, enter `WDC Settings` in the `Quick Find` box, then select **WDC Settings**.

2. Under Thanks Settings, select `Enable`.

3. Click **Save**.

To disable Chatter Thanks, from Setup, enter `WDC Settings` in the `Quick Find` box, then select **WDC Settings** and deselect `Enable`. Users no longer see the Thanks action in the Chatter publisher or in the Salesforce mobile app action bar. However, they can still see previously created Thanks posts.

> **EDITIONS**
>
> Available in: Salesforce Classic and Lighting Experience
>
> Available in: **All Editions** that have Chatter enabled.

Guidelines for Deleting Your Users' Chatter Messages

Salesforce administrators with the Manage Chatter Messages permission can access all users' private messages via SOAP API. You can view and delete any message (for example, for compliance).

When you delete private Chatter messages, consider these guidelines.

*   Messages are hard deleted. That is, they're removed completely without a trip to the Recycle Bin.

*   Deleted messages aren't included in message search results.

*   Deleting a message that resulted from sharing a file with someone doesn't also delete the file.

*   If all messages in a conversation are deleted, the conversation isn't shown in My Messages. The conversation can't be retrieved via Connect REST API.

*   If replies via email are enabled, and a user replies to a deleted message, Chatter returns an error notification and doesn't process the reply message.

> **EDITIONS**
>
> Available in: Salesforce Classic (not available in all orgs)
>
> Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions for users with a Salesforce license, and **Database.com** Edition for users with a Database.com Admin license

Report on Chatter with the Dashboards Package

The Chatter Dashboards package for Salesforce Classic packs a punch! You get multiple dashboards, over 100 reports, and even custom report types. Use the dashboards to monitor and manage Chatter adoption and engagement in your organization.

Use the Salesforce Chatter Dashboards package to:

*   View overall Chatter adoption with detailed metrics and monthly trends

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

- Monitor group adoption with membership and engagement metrics, such as the number of posts, comments, likes, and the top contributors
- Monitor content creation and user engagement, such as the top files, trending content, and the top contributors
- View topic taxonomy and monitor topic assignments, including the most assigned topics and the top assigners
- Create customized reports using existing groupings such as department, country, role, or profile

You can install the Salesforce Chatter Dashboards from AppExchange.

Tip: For installation instructions, detailed information about the reports, and upgrade instructions, see Get Started with Chatter Dashboards.

After the package is installed, you can access your new dashboards, reports, and custom report types alongside all your other Salesforce dashboards and reports.

As newer versions of the package become available, you can upgrade your package by reinstalling it. If you customized any of the reports and dashboards, your customizations are retained during upgrade.

Dashboard	Description
Overview	See the overall state of Chatter at a glance.
Adoption by Department	Get an overview of department metrics for groups, user profiles, and topic adoption.
Files	Track file uploads, downloads, engagement, and content creators.
Groups	Monitor feed and member activity in Chatter groups.
Management	Track unanswered questions and posts, group growth rates, and the overall health of your groups.
Q&A	Track recent activity for questions, answers, and best answers posted in groups.
Topics	Track your Chatter topics activity.
User	Track recent activity for questions, answers, and best answers in user profiles.

Note: The reports in this package return data for all Chatter. If your organization is using an Experience Cloud site, we recommend that you install the Salesforce Communities Management (for Communities with Chatter) package instead. This package allows you to report on Chatter usage in your internal organization and Chatter usage in your site.

Currently, you can't customize a report that is based on records that you're following in Chatter.

Chatter Desktop

Control access to Chatter Desktop and install and configure the Chatter Desktop Managed Version.

Control Access to Chatter Desktop

Chatter Desktop is enabled for most organizations, but administrators can control access to Chatter Desktop.

Install Chatter Desktop Managed Version

Salesforce provides two Chatter Desktop installers: a standard version for individual installations and a managed version for enterprise deployments.

Configure Chatter Desktop Managed Version

Control Chatter Desktop settings by deploying an XML-based configuration file to each user's machine. The configuration in the file overrides the user's settings.

Control Access to Chatter Desktop

Chatter Desktop is enabled for most organizations, but administrators can control access to Chatter Desktop.

> ⊘ **Important:** Chatter Desktop was retired in June 2018. For more information, see Chatter Desktop Retirement.

1. From Setup, enter `Chatter Desktop Settings` in the `Quick Find` box, then select **Chatter Desktop Settings**.

2. To allow users to access Chatter data from Chatter Desktop, select `Enable Chatter Desktop`.

   To block access to the Chatter Desktop self-installation page and prevent all instances of Chatter Desktop from accessing Chatter data, deselect this option.

3. To prevent non-administrators from installing Chatter Desktop, select `Allow Chatter Desktop Managed Installations Only`.

   For example, select this option if your IT department plans to deploy Chatter Desktop to your organization.

4. Save your changes.

SEE ALSO:

Salesforce Chatter

Install Chatter Desktop Managed Version

Configure Chatter Desktop Managed Version

EDITIONS

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

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

Salesforce CRM, Approvals, Chatter email notifications, Chatter Invitations, and customer invitations are not available in **Database.com**.

Install Chatter Desktop Managed Version

Salesforce provides two Chatter Desktop installers: a standard version for individual installations and a managed version for enterprise deployments.

⛔ **Important:** Chatter Desktop was retired in June 2018. For more information, see Chatter Desktop Retirement.

The following are the minimum requirements for using Chatter Desktop:

- Windows
  - 2.33 GHz or faster x86-compatible processor, or Intel Atom™ 1.6 GHz or faster processor for netbook devices
  - Microsoft® Windows® XP, Windows Server® 2003, Windows Server 2008, Windows Vista® Home Premium, Business, Ultimate, or Enterprise (including 64-bit editions) with Service Pack 2, or Windows 7
  - 512 MB of RAM (1 GB recommended)

- Mac
  - Intel® Core™ Duo 1.83 GHz or faster processor
  - Mac OS X v 10.5, 10.6, or v10.7
  - 512 MB of RAM (1 GB recommended)

⛔ **Important:** Chatter Desktop uses Adobe® Integrated Runtime (AIR®), Adobe's cross-platform runtime environment for desktop applications, and runs only on operating systems that Adobe AIR supports. Chatter Desktop doesn't run on operating systems that Adobe AIR doesn't support, such as 64-bit Linux. See the Adobe website for information on Adobe AIR.

The managed version of Chatter Desktop is ideal for enterprises deploying Chatter Desktop to users who don't have administrator privileges on their machines. The managed version:

- Doesn't automatically install AIR. Your IT department must obtain a redistribution agreement from Adobe Systems Incorporated and deploy the required version of AIR before they deploy Chatter Desktop
- Requires your IT department to accept the Chatter Desktop managed version end-user license agreement on behalf of the deployed Chatter Desktop users
- Doesn't automatically post to Chatter when Chatter Desktop first launches
- Doesn't regularly check Salesforce for new versions

To install the managed version:

1. Deploy Adobe® Integrated Runtime (AIR®) version 2.6 or later (the latest version is recommended) to the machines where you plan to deploy Chatter Desktop.

   AIR is Adobe's cross-platform runtime environment for desktop applications, and is a prerequisite for Chatter Desktop.

   💡 **Tip:** Visit these links before deploying AIR:
   - AIR® overview:
     http://www.adobe.com/devnet/air/articles/distributing_air_in_enterprise.html
   - Information on obtaining an AIR® redistribution license from Adobe Systems Incorporated:
     http://www.adobe.com/products/air/runtime_distribution1.html
   - Installation information:
     http://help.adobe.com/en_US/air/redist/WS485a42d56cd19641-70d979a8124ef20a34b-8000.html

- Administration information:
  http://help.adobe.com/en_US/air/admin/WS485a42d56cd1964167ea49bd124ef17d52a-8000.html

2. From Setup, enter *Chatter Desktop Settings* in the `Quick Find` box, then select **Chatter Desktop Settings**.

3. To download the managed version, click the link.

⊘ **Important:** Chatter Desktop uses Adobe® Acrobat® Reader to preview PDF files. Before you preview files with Chatter Desktop, download Adobe Acrobat from Adobe's website, install it, and open it at least once to complete the installation.

SEE ALSO:
Control Access to Chatter Desktop
Configure Chatter Desktop Managed Version

Configure Chatter Desktop Managed Version

Control Chatter Desktop settings by deploying an XML-based configuration file to each user's machine. The configuration in the file overrides the user's settings.

⊘ **Important:** Chatter Desktop was retired in June 2018. For more information, see Chatter Desktop Retirement.

1. Create a file named `.chatterdesktop`, add a `chatterdesktop` parent element with two child elements, `config` and `servers`.

2. Inside the `config` element, create the child elements listed in this table and add a `default` and an `editable` attribute. Each attribute can have the value *true* or *false*.

To make a child element the default setting, set the element's `default` attribute to *true*. To allow users to change a default setting through the user interface, set the element's `editable` attribute to *true*.

Child Element	Description
launchOnStartup	Launches the application on start-up.
minimizeOnClose	Minimizes the application on close.
notifications	Enables pop-up notifications.
criticalAlerts	Enables alerts for new feed posts and comments by highlighting the taskbar icon (Windows) or causing the dock icon to bounce (Mac OS).
bringToForeground	Brings Chatter Desktop to the foreground for new feed posts and comments.
alwaysOnTop	Enables Chatter Desktop to always display in the foreground.
chatWindowToForeground	Enables the chat window to display in the foreground when a new chat is received (Mac only).

Child Element	Description
chatSoundEnabled	Enables sounds for new chats received.
playSoundForEveryMessage	Enables sounds for all chats received.

> 📝 Note: If the `default` attribute is set to *true* for `chatSoundEnabled` and *false* for
> `playSoundForEveryMessage`, a sound plays only for new chats received. If both are set to *true*, a sound plays for
> every chat received. If both are set to *false*, chat sounds are disabled.

3. If your organization uses instances of Salesforce other than Production and Sandbox, specify the servers that host those instances
in separate `server` elements inside the `servers` element.

Inside each `server` element, include the following attributes:

- `label`—The name of the connection as you want it to appear in the user interface.
- `serverUrl`—The URL you use to log in to the instance. The URL must begin with `https://` and end with
  `salesforce.com` or `chatter.com`. For example, if your organization has a European division that you log into from
  `https://emea.salesforce.com`, enter that URL and name the connection *Europe.*.
- `defaultServer`—Set to TRUE to make this server the default instance to which Chatter Desktop connects.

4. Test the `.chatterdesktop` configuration file.

   a. Copy the `.chatterdesktop` configuration file to the user directory on your machine. The user directories are:

- Mac OS—`/Users/<username>`
- Linux—`/home/<username>`

   b. Launch Chatter Desktop and verify that it functions correctly.

5. Copy the `.chatterdesktop` file to the user directory on every machine that is running Chatter Desktop in your organization.

👁 Example: The following is a sample configuration file:

```
<chatterdesktop>
   <config>
      <launchOnStartup default="false"
                        editable="false"/>
      <minimizeOnClose default="false"
                        editable="true"/>
      <notifications default="true"
                        editable="true"/>
      <criticalAlerts default="false"
                        editable="true"/>
      <bringToForeground default="false"
                        editable="true"/>
      <alwaysOnTop default="false"
                        editable="false"/>
      <chatWindowToForeground default="false"
                        editable="false"/>
```

```
        <chatSoundEnabled default="true"
                          editable="true"/>
        <playSoundForEveryMessage default="true"
                          editable="true"/>


    </config>

    <servers>
        <server label="Europe"
                serverUrl="https://emea.salesforce.com"
                defaultServer="true"/>
        <server label="Production"
                serverUrl="https://login.salesforce.com"
                defaultServer="false"/>
    </servers>
</chatterdesktop>
```

SEE ALSO:
   Control Access to Chatter Desktop
   Install Chatter Desktop Managed Version

Salesforce Files

Customize page layouts to include the Files related list, so users see a list of files associated with a record.

Add the Files Related List to Page Layouts
Customize page layouts to include the Files related list. With the Files related list, users can add files to a record and see a list of files associated with the record.

Customize the Files Detail Page
In Lightning Experience, you can customize the fields and layout of the Files detail page. Use record types to customize the layouts of different record types, and tailor the data you capture based on the file type. Choose from standard fields to show when the file was last updated, file size, file type, and more. Create custom fields and buttons to track metadata that's specific to your business, to use in validation rules, and to provide data for searches and reports. Use record types to customize the page layouts of different file record types.

Prevent Users from Attaching Salesforce Files
Use permission sets to prevent users from attaching Salesforce Files to posts, records, and other objects.

Add File Privacy on Records to Edit File Details Layout
Add the File Privacy on Records option to the Edit File Details layout to let file owners control the visibility of files attached to records.

Set File Sharing to Inherit Record Permissions
Set the default sharing permissions on files that are attached to records so that they inherit the sharing settings of the record. When enabled, a user who can edit a record can also edit the files on that record. This setting applies to files attached to records created manually from the Files related list and files attached in the record's Chatter feed.

Configure File Upload and Download Security Settings

To provide more security, control the way some file types are handled during upload and download.

Enable Content Deliveries and Public Links

Use Content deliveries and public links to send links to files to people inside or outside your organization.

Regenerate a File Preview

If a file preview is of poor quality, you can try to regenerate the preview. Available for Salesforce Files and CRM content documents that can be previewed.

Salesforce Files Storage Allocations

Your organization-wide file storage allocation.

Asset Files

Asset files are packageable versions of Salesforce files that are used for branding and design purposes in your org or Experience Cloud site. Asset files can be used for headers and logo images. They can also be referenced by components. You don't need to create asset files for regular, collaborative use of Salesforce Files.

Salesforce Files: What's Different or Not Available in the Salesforce Mobile App

Check out the differences between the desktop version and the mobile version of Salesforce Files.

Add the Files Related List to Page Layouts

Customize page layouts to include the Files related list. With the Files related list, users can add files to a record and see a list of files associated with the record.

Use files instead of attachments to make the files available outside of the context of the individual record. The file owner or admin still decides sharing settings for the file.

1. From Setup, at the top of the page, select **Object Manager** and select the object you want to add the Files related list to (such as Opportunity).

2. Click **Page Layouts**.

3. Click the page layout you want to customize.

4. In the list of available items in the left pane, click **Related Lists**.

5. Drag **Files** to the Related Lists section and click **Save**.

   📝 Note: Users can't drag files to add them to a record when the related list type is **Basic List**. To change the related list type, edit the related list component in the Lightning App Builder.

EDITIONS
Available in: Salesforce Classic (not available in all orgs) and Lightning Experience
Available in: **Group**, **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Contact Manager**, and **Developer** Editions

Customize the Files Detail Page

In Lightning Experience, you can customize the fields and layout of the Files detail page. Use record types to customize the layouts of different record types, and tailor the data you capture based on the file type. Choose from standard fields to show when the file was last updated, file size, file type, and more. Create custom fields and buttons to track metadata that's specific to your business, to use in validation rules, and to provide data for searches and reports. Use record types to customize the page layouts of different file record types.

To see the Files Detail Page, set up at least one custom record type (in addition to General, the default type).

To customize the Files detail page

EDITIONS
Available in: Lightning Experience
Available in: **Essentials**, **Group**, **Enterprise**, **Professional**, **Performance**, **Unlimited**, **Contact Manager**, and **Developer** Editions

1. From Setup, enter *Object Manager* in the Quick Find box, and click **Object Manager**.

2. In the Object Manager, click **Content Version**, then click **Page Layouts**.

3. Create a new page layout or open the existing page layout that you use for the **Edit File Details** page.

These check boxes can be added to the page layout of the edit file detail page:

- **Add File Privacy on Records to Edit File Details Layout** Lets file owners control the visibility of files attached to records.
- **Prevent Others from Sharing and Unsharing a File** Lets file owners prevent others from sharing and unsharing their file. (Checking this box doesn't affect existing shares of a file.)

Note: The custom layout displays when users view or edit file details from the actions arrow on Files home, or edit file details from a file preview. However, from the files related list on a record, clicking **Edit File Details** displays the default file detail page instead of the custom layout. To see the custom file detail page layout on a file attached to a record, click the file title to open the file preview, and then click **Edit File Details**.

From the Content Version object in Object Manager, you can also:

- Create custom fields and buttons to track metadata to use in validation rules and provide data for searches and reports.
- Create validation rules for files added to libraries, records, and Files home. By requiring users to follow naming conventions or fill in mandatory fields, you can improve the quality of the data and metadata in your org.

Prevent Users from Attaching Salesforce Files

Use permission sets to prevent users from attaching Salesforce Files to posts, records, and other objects.

1. From Setup, enter *User Profiles* in the Quick Find box, and select **Profiles**.

2. Click **Edit** next to the user profile you want to change.

3. In the Administrative Permissions section, enable or disable the **Select Files from Salesforce** checkbox, and click **Save**.

Note: Another option is to apply the permission in a permission set. Users who have this permission disabled are still able to upload files from their local drive. To apply the permission in a permission set, from Setup enter *Permission Sets* in the QuickFind box, then select **Permission Sets**. Edit the permission set and apply the Select Files from Salesforce permission.

EDITIONS

Available in: All Editions

Permission sets available in: **Contact Manager**, **Professional**, **Group**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Add File Privacy on Records to Edit File Details Layout

Add the File Privacy on Records option to the Edit File Details layout to let file owners control the visibility of files attached to records.

If you don't see the File Privacy on Records option, you can add it by customizing the Content Version page layout.

> **Note:** In Salesforce Classic, the File Privacy on Records option also appears on the content detail page and in the content edit dialog. If a file is marked as private in Lightning Experience, it's also private in Salesforce Classic. This feature is also available in Experience Cloud sites. Only admins and a file's owner can change the value of File Privacy on Records.

1. From Setup, enter `Object Manager` in the `Quick Find` box, and click **Object Manager**.

2. In the Object Manager, click **Content Version**, then click **Page Layouts**.

3. Open the page layout that you use for the Edit File Details page.

4. In the layout palette, select **Fields**, drag **File Privacy on Records** to the Fields section under Content Detail Version, and click **Save**.

> **Tip:** Though you can place the option anywhere in the Fields section, consider placing it after **Description**.

To see your result, from the Files tab, go to the Files page and edit a file's details.

EDITIONS

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

USER PERMISSIONS

To customize Content Version layouts:
- Customize Application

Note: When you click **Edit File Details from Related Lists**, the File Privacy on Records field isn't visible.

Set File Sharing to Inherit Record Permissions

Set the default sharing permissions on files that are attached to records so that they inherit the sharing settings of the record. When enabled, a user who can edit a record can also edit the files on that record. This setting applies to files attached to records created manually from the Files related list and files attached in the record's Chatter feed.

With this preference enabled:

- Users with read/write access to a record get Collaborator access to attached files.
- Users with read-only record access get Viewer access to attached files.

When the preference is disabled, all files attached to records default to viewer access.

Note: Files uploaded by guest users can only be set to Viewer access.

From Setup, enter `Files` in the QuickFind box. Under Salesforce Files, choose **General Settings**. Enable the preference **Set file access to Set by Record for files attached to records**.

Note:

- Viewers can view, download, and share files.
- Collaborators can view, download, share, edit the file, and upload new versions.
- File owners and collaborators can change file permissions for people and groups.

Configure File Upload and Download Security Settings

To provide more security, control the way some file types are handled during upload and download.

To manage file upload and download settings:

1. From Setup, enter `File Upload and Download Security` in the Quick Find box, then select **File Upload and Download Security**.

2. Click **Edit**.

3. To prevent users from uploading files that can pose a security risk, select `Don't allow HTML uploads as attachments or document records.`

   This setting blocks the upload of these MIME file types: `.html`, `.htt`, `.mht`, `.svg`, `.swf`, `.thtml`, and `.xhtml`.

   ⚠ **Warning:** Keep the following in mind when selecting this option:

   - If your organization uses the partner portal to give your partner users access to Salesforce, we don't recommend enabling this setting. Enabling this setting prevents your organization from customizing the appearance of your partner portal.

   - HTML attachments are not permitted on solutions, regardless of whether this security setting is enabled. In addition, this setting does not affect attachments on email templates; HTML attachments on email templates are always permitted.

   - After this setting is enabled, previously-uploaded HTML documents and attachments are unaffected. However, when users attempt to view an HTML attachment or document, their browser first prompts them to open the file in the browser, save it to their computer, or cancel the action.

4. Set download behavior for each file type:

   a. **Download** (recommended): The file, regardless of file type, is always downloaded.

   b. **Execute in Browser**: The file, regardless of file type, is displayed and executed automatically when accessed in a browser or through an HTTP request.

   c. **Hybrid**: Salesforce Files are downloaded. Attachments and documents execute in the browser.

5. Click **Save**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

USER PERMISSIONS

To configure file upload and download settings:
- Customize Application

Enable Content Deliveries and Public Links

Use Content deliveries and public links to send links to files to people inside or outside your organization.

With content deliveries, you can set a password or an expiration date for the link, and track how frequently the content is viewed. When you create a public link to a file, you can set a password and expiration date. Public links to folders don't have password protection or link expiration. You can't track content views on public links to files or folders.

Any time confidential documents are shared, we recommend requiring password protection.

Other Permissions

EDITIONS

Available in: Lightning Experience

USER PERMISSIONS

To enable content deliveries and public links:
- Customize Application

In addition to the global settings that enable content deliveries and public links for your org, you need to enable the user permissions "Create Content Deliveries" or "Create Public Links" on profiles or in permission sets.

Files in libraries are governed by settings in the library, not user permissions. To share files managed by a library, Deliver Content must be enabled for the user in the library.

After enabling content delivery and choosing a default for password protection, add the Content Deliveries related list to your page layouts to create new content deliveries and find details about existing deliveries on a record.

1. From Setup, enter `Content Deliveries and Public Links` in the `Quick Find` box, and select **Content Deliveries and Public Links**. Select `Content Deliveries feature can be enabled for users` and `Public Links can be enabled for users (Requires Content Deliveries)`.

2. From Setup, enter `Permission Sets` in the `Quick Find` box, and select **Permission Sets**. Select a permission set, click **System Permissions**, and select `Create Public Links`.

3. From Setup, enter `Profiles` in the `Quick Find` box, and select **Profiles**. Select a profile, and click **Edit**. In **General User Permissions**, select `Create Public Links`. You don't need this permission for files in a shared Salesforce CRM Content library. Instead, complete steps 1 and 2 and then ensure that the user is a library member and that **Deliver Content** is checked in the library permission definition.

4. From Setup, enter `Content Permissions` in the `Quick Find` box, and select **Content Permissions**. Next to Library Administrator in the list of library permissions, click **Edit**, enable **Deliver Content**, and save your changes.

Regenerate a File Preview

If a file preview is of poor quality, you can try to regenerate the preview. Available for Salesforce Files and CRM content documents that can be previewed.

When you regenerate a preview, the new preview request is added to a queue and the existing preview is deleted. During this time, users won't see a file preview.

With very large files, only the first 500 pages will render in the preview.

File previews aren't available for files larger than 25 MB, unknown file types, password-protected files, and copy-protected PDFs. For files that you can't preview, the Preview option isn't available on feeds or list views, and files appear as generic file type icons in the feed.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To regenerate a preview:
- Customize Application

To Regenerate a File Preview

1. From Setup, enter `Regenerate Previews` in the Quick Find box, then select **Regenerate Previews**.

2. Specify either the Content Document ID or the Content Version ID. When you specify a Content Document ID but don't specify a the Version Number, the latest version is used.

   📝 Note: To find the Content Document ID, click View File Details from the file menu on Files Home or from the file preview. From the file detail page, the Content Document ID displays in the file URL following the ContentDocument/ section.

To see whether the preview regenerated successfully, navigate to the file detail page.

Salesforce Files Storage Allocations

Your organization-wide file storage allocation.

Shared Organization-Wide Storage

File storage for your org is calculated by a base allocation based on your Salesforce edition plus a per-user allocation multiplied by the number of standard licensed users in your organization.

Salesforce Edition	File Storage Allocation Per Organization	File Storage Allocation Per User License
Contact Manager	10 GB	612 MB
Group	10 GB	612 MB
Professional	10 GB	612 MB
Enterprise	10 GB	2 GB
Performance	10 GB	2 GB
Unlimited	10 GB	2 GB
Developer	20 MB	N/A
Personal	20 MB	N/A

Note: If your Contact Manager, Group, or Professional Edition org has fewer than 10 people, your per-user file storage equals 1 GB.

Note: If your organization uses custom user licenses, contact your administrator to determine if these licenses provide additional storage.

Asset Files

Asset files are packageable versions of Salesforce files that are used for branding and design purposes in your org or Experience Cloud site. Asset files can be used for headers and logo images. They can also be referenced by components. You don't need to create asset files for regular, collaborative use of Salesforce Files.

[Create a New Asset File](#)

Create an asset file from the Asset Library in Files home.

[View and Edit Asset Files](#)

You can view asset files in the Asset Files library in Files home, and view and edit asset files in Setup.

Create a New Asset File

Create an asset file from the Asset Library in Files home.

Salesforce admins and community managers have access to the Asset Library by default. Standard users who are members of the Asset Library can also create asset files.

1. From Files home, go to **Libraries** > **Asset Library**.

2. Click **Upload Asset File**. The file selector opens to let you upload a new file or select an existing file to make into an asset.

3. After you select a file, a dialog window displays these fields:

   - `Asset File Name` - On this screen, this field displays the API Name. After you click **Save**, this field displays the name of the file that you uploaded.

   - `API Name` - The unique name of the asset file in the API, also known as the developer name.

     Note: If you edit the API name, be sure to follow the DeveloperName requirements described in the [ContentAsset](#) object reference.

   - `Let guest users see this asset file on public and login pages` - Select this option to make the asset file visible to guest users on public and login pages. When this option is checked, unauthenticated guest users can see logos and other images on your login page and other public pages.

   - `Make asset file available to Salesforce org users` - Select this option to make this asset file accessible to all internal employees. Leave it unchecked if you prefer to restrict access to asset files.

4. Click **Save**. Your asset file is saved to the Asset Library and displays an Asset File label.

   Note: To see and edit your asset files in Setup, enter `Asset Files` into the `Quick Find` box.

SEE ALSO:

[View and Edit Asset Files](#)

View and Edit Asset Files

You can view asset files in the Asset Files library in Files home, and view and edit asset files in Setup.

Salesforce admins and community managers have access to the Asset Library by default. Admins can edit and delete asset files they don't own. Standard users who are members of the Asset Library can edit and delete only the asset files they own.

View and Edit Asset Files

To view asset files in Files home, select `Libraries` and then select `Asset Library`.

To view and edit asset files in Setup, enter `Asset Files` in the `Quick Find` box, then select **Asset Files**. Click the name of a resource to view its details. Details include who last modified the file, visibility to unauthenticated users, and a link to the file detail page.

From the asset file detail page, you can:

- Edit the asset file.
- Delete the asset file.
- Click **Clone** to create a copy of the asset file, and give it a new name.
- Click **Where is this used?** to view a list of all references to the asset file in your organization.

From the Asset File Edit page, you can:

- Edit the file name.
- Edit the unique API name, also known as the developer name.

    Note: If you edit the API name, be sure to follow the DeveloperName requirements described in the ContentAsset object reference.

- Update the checkbox that allows unauthenticated guest users to see the asset file.
- Update the Master Language associated with the file.

Delete Asset Files

Delete asset files from the asset file detail page. After an asset file is deleted, it exists in the Salesforce cache for up to 24 hours. After 24 hours it is permanently deleted from our systems.

    Note: An asset may still be accessible if it's cached locally by a browser, or cached by an external system.

SEE ALSO:

Create a New Asset File

Salesforce Files: What's Different or Not Available in the Salesforce Mobile App

Check out the differences between the desktop version and the mobile version of Salesforce Files.

    Important: Chatter must be enabled for your org to view, open, and upload files.

When using Salesforce Files in the Salesforce mobile app, you **cannot**:

- Add more than one file to feed items in Chatter
- See multiple files attached to a feed item in the main Chatter feed—only the first attachment is displayed *(Salesforce for Android only)*
- View file types other than these: `.doc`, `.docx`, `.pdf`, `.ppt`, `.pptx`, `.xls`, `.xlsx`, and all image files, including `.gif`, `.jpg`, and `.png` formats
- Create, rename, or delete library folders
- Share a file you have Viewer access to
- Move files in libraries into folders
- Access Files from the navigation menu if you're a high-volume portal user
- Upload files using the Good Access secure mobile browser
- Assign topics to files in the main Chatter feed *(downloadable apps only)*

Content Libraries and Files

The support for Salesforce CRM Content in the Salesforce for iOS is geared towards letting users view and share content. Other activities, such as managing or contributing to libraries, aren't available in the app. Here's how working with content libraries is different from what users can do in the desktop site.

- The Private Library folder isn't available. Instead, a user can access the files in their private library by selecting the Owned by Me filter in the Files list on Files home.
- When viewing libraries, the top content, popular tags, recent activity, and most active contributors sections aren't available.
- Users can't:
    - See content detail pages
    - Upload and publish new or revised files to libraries
    - Publish web links in libraries
    - Edit content details
    - Add, edit, or delete comments
    - Delete files (Salesforce for iOS and Salesforce for Android)
    - Move files to different libraries
    - Use tags to classify or filter content
    - Subscribe to libraries, files, authors, or tags
    - Provide feedback on content, or review feedback on content
    - Delete, archive, or restore content
- Content search options like filtering by file type, author, or library name aren't available. But users can use global search to find files in libraries.
- Creating or managing content deliveries isn't available. This includes generating an encrypted URL for sharing files and content packs with customers.

Salesforce Files Connect

With Files Connect, Salesforce users can access, share, and search external data from systems like Quip, Google Drive, SharePoint, or Box.

The Files Connect Setup Process

The setup process for Files Connect varies by external data source.

Enable Salesforce Files Connect for Your Organization

Let users search and share files from external systems like Google Drive and SharePoint.

Let Users and Administrators Access Files Connect Data Sources

After you enable Files Connect, give users and administrators permission to access specific external data sources from Salesforce.

Create an Authentication Provider for Box

To use Box as an external data source, first create an authentication provider for it in Salesforce.

Define an External Data Source for Box

Let users access their Box content from Files home, feed posts, and search.

Create an Authentication Provider for Google Drive

To use Google Drive as an external data source, create an authentication provider for it in Salesforce. The process begins with creating a related project in the Google Developers console.

Define an External Data Source for Google Drive

Let Chatter users access their Google Drive content from the Files tab, feed posts, and search. Salesforce supports Google documents, spreadsheets, presentations, and drawings.

Create an Authentication Provider for SharePoint Online Using Azure (Preferred Method)

To use a Microsoft cloud-based external data source, create an authentication provider for it in Salesforce and register that provider in a Microsoft Azure web application.

Create an Authentication Provider for SharePoint Online or OneDrive for Business Using Office 365 (Alternate Method)

To use one of Microsoft's cloud-based external data sources, first create an authentication provider for it in Salesforce and register that provider in an Office 365 app.

Define an External Data Source for SharePoint Online or OneDrive for Business

With Files Connect and Chatter, Salesforce can access content from Microsoft's cloud-based systems.

Include a Files Connect Data Source in Global Search

Combine searches for Salesforce data with external data from Google Drive, SharePoint, OneDrive for Business, or Box. Developers can automate the process with supported SOQL or SOSL queries with the API.

Include SharePoint Custom Properties in Search, SOQL, and SOSL Queries

After you create an external object for a SharePoint data source, some special steps are needed to search or query any custom properties it contains.

Define a Simple URL External Data Source

If Chatter is enabled for your organization, Salesforce can access data hosted on another web domain for use in the Files tab and feed.

Considerations for Person or Group Between SharePoint and Salesforce

Note the limitations of two data type fields when using SharePoint Online and Salesforce.

Chatter for SharePoint Is EOL

As of the Summer '17 release, Salesforce Chatter for SharePoint reached end-of-life and is no longer supported. Chatter for SharePoint was a SharePoint plugin that let users access Chatter feeds from within SharePoint 2010. Salesforce has moved away from this solution to focus its development efforts on other user productivity capabilities. As you move away from the SharePoint plugin, there's no need to worry about data loss. All Chatter data continues to reside securely in the Salesforce org.

The Files Connect Setup Process

The setup process for Files Connect varies by external data source.

> 💡 **Tip:** For detailed visuals, tips, and troubleshooting, see the Files Connect *Setup Guide* and *User Guide*.

First, enable Files Connect, and let users access related external data sources

1. Enable Salesforce Files Connect for Your Organization.

2. Let Users and Administrators Access Files Connect Data Sources.

For cloud-based data sources, create an authentication provider, and then define the source

If you use Google Drive:

1. Create an Authentication Provider for Google Drive.

2. Define an External Data Source for Google Drive.

If you use Quip:

1. Set Up Salesforce Anywhere Advanced.

If you use Microsoft's cloud systems:

1. Create an Authentication Provider for SharePoint Online Using Azure (Preferred Method).

2. Define an External Data Source for SharePoint Online or OneDrive for Business.

If you use Box:

1. Create an Authentication Provider for Box.

2. Define an External Data Source for Box.

Include the external data in global search

To let users access external data in global Salesforce searches, you'll need to create an external object and give users access to its fields. This is an optional step, but highly recommended to best integrate external data with Salesforce.

For per-user data sources, have users authenticate in Salesforce

If you specified per-user authentication for a data source and exposed it through profiles or permission sets, ask authorized users to provide their data source credentials.

Start accessing, sharing, and searching external files!

Now users can access and share external files via the Files tab and feed, and search for them right alongside their Salesforce content.

Enable Salesforce Files Connect for Your Organization

Let users search and share files from external systems like Google Drive and SharePoint.

1. From Setup, enter `Files Connect` in the `Quick Find` box, and then select **Files Connect**.

2. Click **Edit**, and then select **Enable Files Connect**.

3. For File Sharing, select one of the following:

   - **Copy** — stores a copy of external files in Salesforce. If files are shared with a Chatter group, all group members can access the files, even if they lack access to the external system.

   - **Reference** — points to external files stored outside Salesforce. No file previews are available, and file downloads require user access to the external system. (Users must enter credentials for the system in the Authentication Settings for External Systems section of personal setup).

   💡 Tip: Choose Copy mode if your organization shares files with external customers or partners. Choose Reference mode to reflect access restrictions from the external system in Salesforce.

Regardless of sharing mode, files in Salesforce don't reflect file revisions in external systems. However, Reference mode points to the latest versions in those systems.

SEE ALSO:
  The Files Connect Setup Process
  Let Users and Administrators Access Files Connect Data Sources

EDITIONS

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

Files Connect for cloud-based external data sources is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To enable Salesforce Files Connect:
- Customize Application

Let Users and Administrators Access Files Connect Data Sources

After you enable Files Connect, give users and administrators permission to access specific external data sources from Salesforce.

💡 Tip: You can provide access to data sources through permission sets or custom profiles. However, permission sets let you more quickly adjust access for several types of users. Regardless of which method you choose, be sure to give administrators access so they can configure data sources.

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. Create a permission set or profile, or click an existing one.

   If you use a permission set, User License must be set to the default option, "None."

3. For a permission set, click **System Permissions**, then click **Edit**.

   For a profile, click **Edit**, and scroll down to the Administrative Permissions section.

4. To access cloud-based data sources, select **Files Connect Cloud**, and then click **Save**.

5. For a permission set, click **Manage Assignments** in the toolbar at the top of the page. Then click **Add Assignments**, select users for the permission set, and click **Assign**.

   ⛔ Important: Include any administrators who need to configure external data sources.

EDITIONS

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

Files Connect for cloud-based external data sources is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To set permissions:
- Customize Application

6. If you haven't already, define the external data sources for your organization:

- Define an External Data Source for SharePoint Online or OneDrive for Business
- Define an External Data Source for Google Drive
- Define an External Data Source for Box

  📝 Note: If you select an identity type of Named Principal for the data source, skip the following steps. But if you select Per User, read on.

7. In Setup, return to the detail page for the permission set or profile. Then do either of the following:

- For a permission set, in the Apps section, click **External Data Source Access**.
- For a profile, go to the Enabled External Data Source Access related list.

8. Click **Edit**, add specific data sources to the Enabled External Data Sources list, and click **Save**.

(Users enter their credentials when they first access external data sources, or from their personal settings on the Authenticated Settings for External Systems page.)

SEE ALSO:
   The Files Connect Setup Process
   Enable Salesforce Files Connect for Your Organization

Create an Authentication Provider for Box

To use Box as an external data source, first create an authentication provider for it in Salesforce.

💡 Tip: For detailed visuals, tips, and troubleshooting, see the Files Connect *Setup Guide* and *User Guide*.

Create an Authentication Provider in Salesforce

1. In Setup, enter `Auth. Providers` in the `Quick Find` box, then select **Auth. Providers**.

2. Click **New**.

3. For `Provider Type`, select **OpenID Connect**, and then set the following options:

- `Name` — Enter the name you want to appear in Salesforce.
- `URL Suffix` — Enter a suffix you want to appear at the end of the URL path. By default, the suffix reflects the Name entry.
- `Consumer Key` — Enter any placeholder value. You fill this in after you create the Box application in Step 5.
- `Consumer Secret` — Enter any placeholder value. You fill this in after you create the Box application in Step 5.
- `Authorize Endpoint URL` — Enter https://account.box.com/api/oauth2/authorize
- `Token Endpoint URL` — Enter https://api.box.com/oauth2/token
- `User Info Endpoint URL` — Leave empty.
- `Default Scopes` — Leave empty.

EDITIONS

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

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

USER PERMISSIONS

To create authentication providers:
- Customize Application

  AND

  Manage Auth. Providers

---

4. Click **Save**. Then, at the bottom of the Auth. Provider detail page, copy the `Callback URL` entry to a text file. (Use this when creating the Box application.)

5. Create a Box application. Then continue to step 6.

6. After you create the Box application, edit the Salesforce Auth. Provider and replace the following values with those from the Box app.

   - `Consumer.Key`: the Box client_id.
   - `Consumer.Secret`: the Box client_secret.

7. Click **Save**.

   Your Box authentication provider is now ready to use.

Create a Box Application

1. Using the credentials of your Box admin account, log in to `https://app.box.com/developers/services`.

2. Click **Create a Box Application**.

3. Enter a project name, select Box content, and click **Create Application**.

4. Click **Configure your application**.

5. In the **redirect_uri** field, paste the Salesforce callback URL specified in the OAuth2 specification.

6. Copy the **client_id** and **client_secret** values to a text file. Enter these values at step 6 of Create an Authentication Provider in Salesforce.

Define an External Data Source for Box

Let users access their Box content from Files home, feed posts, and search.

1. From Setup in Salesforce Classic, enter `External Data Sources` in the `Quick Find` box, then select **External Data Sources**.

2. Click **New External Data Source**. Then set the following options.

Field	Description
Label	A user-friendly name for the data source displayed in the Salesforce user interface.
Name	A unique identifier used to refer to this external data source definition through the API. The **Name** field 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.
Type	Choose **Files Connect: Box**

Field	Description
`Identity Type`	The identity type used to authenticate to the external data source. Select **Per User** to require separate credentials for each user who accesses the data source. (Administrators must enable the data source for specific permission sets and profiles. Users then enter their credentials when first accessing the data source.)
`Authentication Protocol`	The protocol used to access Box. Select **OAuth 2.0**.
`Authentication Provider`	Enter the Box Authentication Provider.
`Scope`	Leave blank.
`Start Authentication Flow on Save`	Select to immediately test the settings above.

> **Note:** Files from a Box data source can't be previewed in the file preview player.

Create an Authentication Provider for Google Drive

To use Google Drive as an external data source, create an authentication provider for it in Salesforce. The process begins with creating a related project in the Google Developers console.

> **Tip:** For detailed visuals, tips, and troubleshooting, see the Files Connect *Setup Guide* and *User Guide*.

Create a Project in the Google Developers Console

1. Using the credentials of your Google App for Work admin account, log in to **https://console.cloud.google.com**.
2. In the title bar, expand **Select Project** and click **Create Project**.
3. Enter a project name and location, and click **Create**.
4. In the project dashboard, click the menu icon in the upper left, and then click **APIs & Services**.
5. In the API manager, go to the Library tab and search for `Google Drive API`.
6. In the search results, click **Google Drive API**, and then click **Enable API**.
7. In the menu on the left, click **Credentials**.
8. In the OAuth Consent Screen tab, enter a valid email address and application name, and click **Save**.
9. In the Credentials tab, click **Add credentials**, and select `OAuth client ID`.
10. Select `Web application`, and click **Create**.
11. Copy the client ID and client secret values to a text file. Use these values when creating an authentication provider in Salesforce.

Create an Authentication Provider in Salesforce

1. In Setup, enter `Auth. Providers` in the `Quick Find` box, then select **Auth. Providers**.

2. Click **New**.

3. For `Provider Type`, select **OpenID Connect**, and then set the following options:

    *   `Name` — Enter the name you want to appear in Salesforce.

    *   `URL Suffix` — Enter the suffix at the end of the URL path. For example, in the path,
        `https://login.salesforce.com/services/authcallback/00Dx00000000001/MyGoogleProvider`,
        the suffix is "MyGoogleProvider"

    *   `Consumer Key` — Enter the client ID you copied when creating the Google project.

    *   `Consumer Secret` — Enter the client secret you copied when creating the Google project.

    *   `Authorize Endpoint URL` —Enter
        `https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force`

    *   `Token Endpoint URL` — Enter `https://accounts.google.com/o/oauth2/token`

    *   `Default Scopes` — Enter `openid email profile https://www.googleapis.com/auth/drive`

4. Click **Save**. Then, at the bottom of the Auth. Provider detail page, copy the `Callback URL` entry to a text file. (Use this URL when editing the Google project.)

Edit the Project in the Google Developer Console

1. In the API Manager, in the menu on the left, click **Credentials**.

2. Click the previously created web app.

3. In the Authorized Redirect URIs section, add the Callback URL you copied when creating the authentication provider in Salesforce, and click **Save**.

Define an External Data Source for Google Drive

Let Chatter users access their Google Drive content from the Files tab, feed posts, and search. Salesforce supports Google documents, spreadsheets, presentations, and drawings.

1. From Setup, enter `External Data Sources` in the `Quick Find` box, then select **External Data Sources**.

2. Click **New External Data Source**. Then set the following options.

Field	Description
Label	A user-friendly name for the data source displayed in the Salesforce user interface.
Name	A unique identifier used to refer to this external data source definition through the API. The **Name** field 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.

Field	Description
Type	Choose **Files Connect: Google Drive**
Identity Type	The identity type used to authenticate to the external data source.
	Select **Per User** to require separate credentials for each user who accesses the data source. (Administrators must enable the data source for specific permission sets and profiles. Users then enter their credentials when first accessing the data source..)
	Select **Named Principal** to use the same set of credentials for every user who accesses the data source from Salesforce.
Authentication Protocol	The protocol used to access Google Drive.
	Select **OAuth 2.0**.
Authentication Provider	Enter the Google Drive authentication provider.
Scope	Leave blank.
Start Authentication Flow on Save	Select to immediately test the settings above.

Create an Authentication Provider for SharePoint Online Using Azure (Preferred Method)

To use a Microsoft cloud-based external data source, create an authentication provider for it in Salesforce and register that provider in a Microsoft Azure web application.

💡 Tip: For detailed visuals, tips, and troubleshooting, see the Files Connect *Setup Guide* and *User Guide*.

To fully configure an authentication provider, complete these steps.

1. Create an Authentication Provider Using Placeholder Values.

2. Register a Web Application in the Azure Management Console.

   📝 Note: If you don't have access to the Azure Management Console, or to authenticate to OneDrive for Business, follow these instructions to register your app in Office 365: Create an Authentication Provider for SharePoint Online or OneDrive for Business Using Office 365 (Alternate Method).

3. Configure the Authentication Provider in Salesforce

Create an Authentication Provider Using Placeholder Values

The authentication provider has a redirect URI so you can register your app.

1. In Setup, enter `Auth. Providers` in the `Quick Find` box, then select **Auth. Providers**.

2. Click **New**.

3. For `Provider Type`, select **OpenID Connect**, and then set the following options.

- `Name` — Enter the name you want to appear in Salesforce.
- `URL Suffix` — Enter a suffix you want to appear at the end of the URL path. By default, the suffix reflects the Name entry.
- `Consumer Key` — Enter a placeholder value.
- `Consumer Secret` — Enter a placeholder value.
- `Authorize Endpoint URL` — Enter a placeholder that begins with *https*.
- `Token Endpoint URL` — Enter a placeholder that begins with *https*.
- `Default Scopes` — Leave empty.

4. Click **Save**. Then, at the bottom of the Auth. Provider detail page, copy the `Callback URL` entry to a text file.

Register a Web Application in the Azure Management Console

1. Log in to Azure at `https://portal.azure.com/`. (If you have any trouble, connect to Azure with your browser in "incognito" mode.)
2. Under **Azure Services**, select **Azure Active Directory**.
3. Select your active directory. Skip this step if you only have one.
4. On the Active Directory page, select **App registrations** from the left navigation menu.
5. In the header menu, click **New Registration**.
6. Under **Create**, enter the following properties:
   - `Name` — Enter a name for your application.
   - `Supported Account Types` — Enter accounts that are only in this organizational directory.
7. Click **Register**.
8. After the app is created, from the left panel, click **Overview**.
9. Copy the `Application ID` to a text file. You need this ID to configure the auth. provider in Salesforce.
10. From the left panel, click **Certificates & Secrets**.
11. Click **New Client Secret**, enter a description, select a duration, and click **Add**. To see the key value, click **Save**.
12. Copy the key so you can use it in the auth. provider.
13. From the left panel, click **Authentication**. Under **Redirect URIs**, select type as **Web** and paste the callback URL that you copied from the bottom of the Auth. Provider detail page.
14. From the left panel, click **API Permissions**, click **Add a permission**, and click **Sharepoint**.
15. Choose which required app permissions you want to enable and click **Add permission**.

Configure the Authentication Provider in Salesforce

In Salesforce, replace the original placeholder values with the correct ones from the Azure app.

1. In Setup, enter `Auth. Providers` in the `Quick Find` box, then select **Auth. Providers**.
2. Next to the authentication provider you created earlier, click **Edit**.
3. Change the following values.
   - `Consumer Key` — Enter the Client ID you copied to a text file.
   - `Consumer Secret` — Enter the key you copied to a text file.

- `Authorize Endpoint URL` — Enter:
  https://login.microsoftonline.com/common/oauth2/authorize?resource=https%3A%2F%2FYOUR_TENANT.sharepoint.com&prompt=login

- `Token Endpoint URL` — Enter: `https://login.microsoftonline.com/common/oauth2/token`

- **SharePoint Online example**
  ```
  https://login.microsoftonline.com/common/oauth2/authorize?prompt=consent&
  resource=https%3A%2F%2Fcontenthubblitz.sharepoint.com%2F
  ```

4. Click **Save**.

   Your authentication provider is now ready to use.

SEE ALSO:

The Files Connect Setup Process

Create an Authentication Provider for SharePoint Online or OneDrive for Business Using Office 365 (Alternate Method)

To use one of Microsoft's cloud-based external data sources, first create an authentication provider for it in Salesforce and register that provider in an Office 365 app.

> 💡 Tip: For detailed visuals, tips, and troubleshooting, see the Files Connect Setup Guide and User Guide.

To fully configure an authentication provider, complete these steps.

1. Create an Authentication Provider Using Placeholder Values

2. Register an Office 365 App

   If you have access to the Azure Management Console, you can register your provider using Azure: Create an Authentication Provider for SharePoint Online Using Azure (Preferred Method) on page 64

3. Edit the Authentication Provider in Salesforce

Create an Authentication Provider Using Placeholder Values

1. In Setup, enter *Auth. Providers* in the Quick Find box, then select **Auth. Providers**.

2. Click **New**.

3. For `Provider Type`, select **Microsoft Access Control Service**, and then set the following options.

   - `Name` — Enter the name you want to appear in Salesforce.

   - `URL Suffix` — Enter a suffix you want to appear at the end of the URL path. By default, the suffix reflects the `Name` entry.

   - `Consumer Key` — Enter a placeholder value.

   - `Consumer Secret` — Enter a placeholder value.

   - `Authorize Endpoint URL` — Enter a placeholder that begins with *https*.

   - `Token Endpoint URL` — Enter a placeholder that begins with *https*.

   - `Default Scopes` — Leave empty.

4. Click **Save**. Then, at the bottom of the Auth. Provider detail page, copy the `Callback URL` entry to a text file. (Use this when registering an Office 365 app.)

Register an Office 365 App

1. Log in to your Office365 account as an administrator, and go to one of the following URLs.

SharePoint Online
```
https://your company name.sharepoint.com/site collection
path/_layouts/15/appregnew.aspx
```

OneDrive for Business
```
https://your company name-my.sharepoint.com/_layouts/15/appregnew.aspx
```

2. Set the following options.

- `Client Id` — Click **Generate**, and copy the generated value to a text file.
- `Client Secret` — Click **Generate**, and copy the generated value to a text file.
- `Title` — Enter a name for the app.
- `App Domain` — Enter the domain name of your Salesforce org.
- `Redirect URL` — Enter the Callback URL you copied when creating the Authentication Provider in Salesforce.

3. Click **Create**.

Now you configure the newly created app to access SharePoint resources.

4. Go to one of the following URLs.

SharePoint Online
```
https://your company name.sharepoint.com/site collection
path/_layouts/15/appinv.aspx
```

OneDrive for Business
```
https://your company name-my.sharepoint.com/_layouts/15/appinv.aspx
```

5. Set the following options.

- `App Id` — Enter the Client Id you copied to a text file, then click **Lookup**.
- `Title` — Keep the default value.
- `App Domain` — Keep the default value.
- `Redirect URL` — Keep the default value.
- `Permission Request XML` — Enter a string with this format.

  SharePoint Online

  ```
  <AppPermissionRequests>
   <AppPermissionRequest Scope="[SCOPE]" Right="[PLACEHOLDER]"/>
  </AppPermissionRequests>
  ```

  OneDrive for Business

  ```
  <AppPermissionRequests>
   <AppPermissionRequest Scope="http://sharepoint/content/tenant"
  Right="[PLACEHOLDER]"/>
  ```

```
<AppPermissionRequest Scope="http://sharepoint/social/tenant" Right="Read"/>
</AppPermissionRequests>
```

6. For SharePoint Online, replace [SCOPE] with one of these values.

   🛇 **Important:** Office 365 recognizes only these scope URLs; copy them exactly, without changes.

   - `http://sharepoint/content/sitecollection/web` so users can access a single site (but not its subsites).
   - `http://sharepoint/content/sitecollection` so users can access a single site collection (including all subsites).
   - `http://sharepoint/content/tenant` so users can access all site collections.

7. Replace [PLACEHOLDER] with one of these values:

   - `Read`
   - `Write`
   - `Manage`
   - `FullControl`

   For details about the differences between permission levels above, see the Microsoft website.

8. Click **Create**.

Edit the Authentication Provider in Salesforce

In Salesforce, replace the original placeholder values with the correct ones from the Office 365 app.

1. In Setup, enter `Auth. Providers` in the `Quick Find` box, then select **Auth. Providers**.

2. Click **Edit** next to the authentication provider you created previously.

3. Change the following values:

   - `Consumer Key` — Enter the Client ID you copied to a text file.
   - `Consumer Secret` — Enter the Client Secret you copied to a text file.
   - `Authorize Endpoint URL` — Enter the URL of the OAuthAuthorize.aspx page in Office 365. The URL format is as follows.

     SharePoint Online
     ```
     https://your company name.sharepoint.com/site collection
     path/_layouts/15/OauthAuthorize.aspx
     ```

     OneDrive for Business
     ```
     https://your company name-my.sharepoint.com/_layouts/15/OauthAuthorize.aspx
     ```

   - `Token Endpoint URL` — Enter a URL in the following format.

     SharePoint Online
     ```
     https://accounts.accesscontrol.windows.net/your company
     name.onmicrosoft.com/tokens/OAuth/2?resource=00000003-0000-0ff1-ce00-000000000000/your
     company name.sharepoint.com@your company name.onmicrosoft.com
     ```

     OneDrive for Business
     ```
     https://accounts.accesscontrol.windows.net/your company
     name.onmicrosoft.com/tokens/OAuth/2?resource=00000003-0000-0ff1-ce00-000000000000/your
     company name-my.sharepoint.com@your company name.onmicrosoft.com
     ```

4. Click **Save**. Your authentication provider is now ready to use.

Define an External Data Source for SharePoint Online or OneDrive for Business

With Files Connect and Chatter, Salesforce can access content from Microsoft's cloud-based systems.

1. From Setup, enter `External Data Sources` in the `Quick Find` box, then select **External Data Sources**.

2. Click **New External Data Source**. Then set the following options.

Field	Description
Label	A user-friendly name for the data source displayed in the Salesforce user interface.
Name	A unique identifier used to refer to this external data source definition through the API. The **Name** field 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. ⊘ Important: This entry must match the value entered in the SharePoint fields, **Managed Properties** > **Property Name** and **Alias**.
Type	Choose **Files Connect: Microsoft SharePoint Online** or **Files Connect: Microsoft OneDrive for Business**.
Site URL	The URL of your SharePoint site, site collection, or web app. ⊘ Important: The URL must begin with *https*. It should look like this: `https://salesforce.sharepoint.com/HRSite` (Don't copy the URL seen in the browser when accessing SharePoint. It should not look like this: `https://salesforce.sharepoint.com/HRSite/SitePages/Home.aspx`)
Exclude Other Site Collections	Accesses only the site collection specified by the URL, ignoring any other site collections. This should always be enabled if any users are

Field	Description
	currently allowed to access the root site collection.
Identity Type	The identity type used to authenticate to the external data source.
	Select **Per User** to require separate credentials for each user who accesses the data source. (Administrators must enable the data source for specific permission sets and profiles. Users then enter their credentials when first accessing the data source.)
	Select **Named Principal** to use the same set of credentials for every user who accesses the data source from Salesforce.
Authentication Protocol	The protocol used to access SharePoint Online.
	Select **OAuth 2.0**.
Authentication Provider	Enter the SharePoint Online or OneDrive for Business authentication provider.
Scope	Leave blank.
Start Authentication Flow on Save	Select to immediately test your settings or to create an external object for this external data source.

> Note: Custom columns defined on SharePoint should not have spaces in the name. Files from a SharePoint Online or OneDrive for Business data source can't be previewed in the file preview player.

SEE ALSO:

The Files Connect Setup Process

Include a Files Connect Data Source in Global Search

Combine searches for Salesforce data with external data from Google Drive, SharePoint, OneDrive for Business, or Box. Developers can automate the process with supported SOQL or SOSL queries with the API.

To include external data in global searches or API queries, first create a related external object. External objects behave similarly to custom objects, but map to data stored outside Salesforce in an external system like SharePoint. Each external object maps to a data table, and the object fields map to accessible table columns.

> 💡 **Tip:** External objects support lookup relationships similar to custom objects, letting you integrate external data into related lists and other areas throughout Salesforce. For details, see External Object Relationships.

To fully configure global search, complete these steps:

1. Choose the Layout for Global Search Results

2. Create an External Object from an External Data Source

3. Give Users Access to the External Object Fields

4. Create a Custom Tab for the External Object (Lightning Experience Only)

To automate search with SOQL or SOSL, review the supported queries for your data source:

- SOQL and SOSL Support for SharePoint and OneDrive External Objects

- SOQL and SOSL Support for Google Drive External Objects

Choose the Layout for Global Search Results

By default, Files Connect external objects use the standard search results layout for Chatter and the Files tab. If you want to display customized search layouts for these objects, complete these steps.

1. From Setup, enter `Files Connect Settings` in the `Quick Find` box, and select **Files Connect Settings**.

2. Select **Use External Object Search Layout**.

Create an External Object from an External Data Source

1. Define an external data source that supports search:

   - SharePoint Online or OneDrive for Business

   - Google Drive

   - Box

2. From Setup, enter `External Data Sources` in the `Quick Find` box, and select **External Data Sources**.

3. To access the details page, click the data source name.

4. Click **Validate and Sync**.

   > 📝 **Note:** Note: If the **Validate and Sync** button is disabled, edit the **Authentication Settings for External Systems** to enable the `Start Authentication Flow on Save` checkbox.

5. Select the table named "items_[data source]." Then, click **Sync** and create an external object that maps to the entire source.

   Now deploy the object to make the data it contains available to users.

6. Choose **Build** > **Develop** > **External Objects**.

7. Click **Edit** next to the new external object.

8. At the bottom of the page, click **Deployed**, and then click **Save**.

Give Users Access to the External Object Fields

1. From Setup, enter *Permission Sets* in the Quick Find box, and select **Permission Sets**.

2. Click a permission set in which you enabled Files Connect.

3. In the Apps section, click **Object Settings**.

4. Click the name of the external object.

5. Click **Edit**, and enable the necessary Read permissions (for the object itself, and all fields you want to reveal in Salesforce).

6. Click **Save**.

Create a Custom Tab for the External Object (Lightning Experience Only)

1. From Setup, enter *Tabs* in the search bar, and select **Tabs**.

2. Click **New** in the Custom Object Tabs section.

3. In Step 1 of the setup wizard, enter the name of the custom object you created from your external data source.

4. In Step 2, choose the availability and visibility of the tab to profiles. The tab doesn't need to be visible, but it does need to be accessible. Choose either **Default On** or **Tab Hidden**.

5. Complete Step 3 and click **Save**.

SOQL and SOSL Support for SharePoint and OneDrive External Objects

SharePoint and OneDrive external objects support these standard fields and any custom fields you enable.

Note: Queries on specific fields return only documents that the external data source indexed.

Field Name	Queryable	Sortable
Author	Yes	Yes
Comment	No	Yes
ContentLength	Yes	Yes
CreationDate	Yes	Yes
DisplayUrl	No	Yes
DownloadUrl	No	No
ExternalId	Yes	Yes
IsFolder	Yes	Yes
MimeType	Yes	Yes
Name	Yes	Yes

Field Name	Queryable	Sortable
UpdateDate	Yes	Yes
UpdatedBy	Yes	Yes

📝 **Note:** You can also use `ParentId_c` as query criteria to retrieve the list of documents in a folder. However, that field isn't displayed in query results unless your query specifies a `ParentId__c` value.

SOQL and SOSL Support for Google Drive External Objects

Files Connect supports all standard Google Drive properties, but not custom properties. The following properties have different field names in Salesforce external objects:

Google Property	Salesforce Field
alternateLink	DisplayUrl
createDate	CreationDate
description	Comment
downloadURL	contentStreamUri
editable	readOnly
fileSize	ContentLength
id	ExternalId
lastModifyingUserName	UpdatedBy
mimeType	MimeType
modifiedDate	UpdateDate
ownerNames	Author
originalFilename	contentStreamFileName
title	Name

This subset of fields supports SOQL and SOSL queries. (None are sortable, reflecting limitations in the Google Drive API.)

- `CreationDate`
- `lastViewedByMeDate`
- `MimeType`
- `Name`

    📝 **Note:** Google Drive queries on the `Name` field support only one wildcard, %. Searches using this wildcard match only name prefixes. For example, the title "HelloWorld" would be returned with the query *Name LIKE "Hello%"* but not *Name LIKE "%World"*.

- `sharedWithMe`

73

> 📝 **Note:** Queries on the `sharedWithMe` field with a value of "false" are not supported, protecting confidential data.

- `starred`
- `UpdateDate`

Include SharePoint Custom Properties in Search, SOQL, and SOSL Queries

After you create an external object for a SharePoint data source, some special steps are needed to search or query any custom properties it contains.

Configuring Custom Properties in SharePoint

If you have the existing mapped custom columns and Office documents' (Microsoft Word, Excel, etc.) metadata in SharePoint, external objects in Salesforce let you select and filter on the following custom properties:

- Custom columns defined in a Custom Content Type
- Metadata from Microsoft Word, Excel, and other Office documents

To search on these custom properties in Salesforce, a Sharepoint administrator must create a corresponding Managed Property.

- To display these properties in external object fields, or use them in SOQL or SOSL `SELECT` queries, set the corresponding Managed Property to `Retrievable`.
- To filter on these properties in external objects, or use them as query criteria in a SOQL or SOSL `WHERE` clause, set the corresponding Managed Property to `Queryable`.

Querying Resulting Fields in Salesforce

In the following example, `CustomProperty` stands for the Custom column name defined in the Custom Content Type, or the Office document metadata name. `ManagedCustomProperty` stands for the corresponding Managed Property name.

SharePoint Online

In most cases, you can use `ManagedCustomProperty` for both the `SELECT` and `WHERE` clause.

Here's a SOQL example:

```
SELECT ManagedCustomProperty FROM items_spOnline_x WHERE ManagedCustomProperty=...
```

However, for file types that SharePoint doesn't index for search, such as .jpg, .png, and .pdf files, you must use `CustomProperty` in the `SELECT` clause and `ManagedCustomProperty` in the `WHERE` clause. As a workaround, you can define an alias on the Managed Property in SharePoint and format queries like this:

```
SELECT Alias FROM items_spOnline WHERE Alias=...
```

> 💡 **Tip:** Normally, custom properties aren't displayed on external object detail pages—defining an alias also addresses this issue.

EDITIONS

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

Files Connect for cloud-based external data sources is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To create an external object and provide access to its fields:
- Customize Application

Boolean Custom Properties

When using boolean (Yes/No) custom properties with a corresponding Managed Property set to the Text type, the corresponding external object field must be set to the Text type as well. In filters, the values "0" and "1" equal false and true, respectively. For example:

```
WHERE customBooleanWithTextManagedProperty="1"
```

"0" and "1" are also displayed as results, however, so boolean custom properties should use a Managed Property type of YesNo. Set the corresponding external object field to Checkbox to query it with standard `true` or `false` values. For example:

```
WHERE customBooleanWithYesNoManagedProperty=true
```

Metadata in Microsoft Office Documents

The Sharepoint Search service returns all metadata from Office documents as strings, so corresponding external object fields must be set to the Text type.

Dates are returned in the format, MM/DD/YYYY hh:mm:ss AM/PM, (for example, "3/31/2015 9:59:00 PM"). To query on fields using the Date type, the external object must include a corresponding Date field for filtering, and a Text field for selecting.

Limitations for Specific SharePoint Property Types in Salesforce

SharePoint Online

- Number, Currency, and Choice multiple properties can't be selected for file types SharePoint doesn't index for search. By default, this includes image, video, and .pdf files, although .pdf files are natively indexed starting with SharePoint 2013.
- Multiple Line of Text, URL, and Date properties aren't queryable.
- Choice multiple and URL properties can't be selected.

SEE ALSO:

Include a Files Connect Data Source in Global Search

Define a Simple URL External Data Source

If Chatter is enabled for your organization, Salesforce can access data hosted on another web domain for use in the Files tab and feed.

1. From Setup, enter *External Data Sources* in the Quick Find box, and then select **External Data Sources**.
2. Click **New External Data Source**, and set the following options:

Field	Description
Label	A user-friendly name for the data source displayed in the Salesforce user interface.

75

Field	Description
Name	A unique identifier used to refer to this external data source definition through the API. The **Name** field 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.
Type	Choose **Simple URL**.
URL	The URL of the server hosting data outside of Salesforce, which must begin with *http://* or *https://*.
Default External Repository	Used for SharePoint® Online®. If metadata is not accessible, use this field to create tables and default table fields.
Large Icon	Specify an icon to easily identify the data source in the Salesforce user interface. First define the icon as a static resource in Salesforce. For more information, see Defining Static Resources.
Small Icon	Specify an icon to easily identify the data source in the Salesforce user interface. First define the icon as a static resource in Salesforce. For more information, see Defining Static Resources.
Identity Type	The identity type used to authenticate to the external data source. Select **Anonymous**, which doesn't require users to provide credentials when accessing the data source.
Authentication Protocol	The protocol required to access the data source. Select **No Authentication**.

> **Note:**
> - Simple URL data sources can't be included in global search, so the "Validate and Sync" option isn't supported.
> - SOQL queries can't be performed on the external objects created from Simple URL data sources.
> - Files from a Simple URL data source can't be previewed in the file preview player.

Considerations for Person or Group Between SharePoint and Salesforce

Note the limitations of two data type fields when using SharePoint Online and Salesforce.

- The SharePoint Online "Lookup (multi-select)" data type with text
- The SharePoint Online "Person or Group" data type with indirect lookup data

If you use these data type columns in SharePoint Online, the column values from SharePoint are not returned to Salesforce.

Chatter for SharePoint Is EOL

As of the Summer '17 release, Salesforce Chatter for SharePoint reached end-of-life and is no longer supported. Chatter for SharePoint was a SharePoint plugin that let users access Chatter feeds from within SharePoint 2010. Salesforce has moved away from this solution to focus its development efforts on other user productivity capabilities. As you move away from the SharePoint plugin, there's no need to worry about data loss. All Chatter data continues to reside securely in the Salesforce org.

📝 Note: We removed the Chatter for SharePoint download from Setup in the Winter '16 release. Going forward, the connection from SharePoint to the Salesforce org Chatter feed doesn't function. So, existing users who try to access the plugin get an error message.

To identify users who have the plugin, search in SharePoint for users with access to pages where the Chatter for SharePoint plugin is deployed.

If you want to replace Chatter for SharePoint, we recommend that you move to SharePointAdept Chatter for SharePoint. A usage note, though: SharePointAdept doesn't create Files Connect file references.

Alternatively, you can build a custom integration using the Chatter public API.

If you have questions, you can reach us by filing a case with Salesforce Support through Salesforce Help.

Salesforce CRM Content

Store, share, and manage your files in content libraries.

Set Up Salesforce CRM Content
Set up Salesforce CRM Content in your org to enable content libraries and set up permissions.

Customize Salesforce CRM Content
Modify content fields, validation rules, library permissions, and other default settings.

Customize Content Fields
Create, modify, and delete Salesforce CRM Content custom fields so you can categorize and define your content.

Libraries
Store, share, and manage your files in content libraries.

Content Settings
Customize content settings and enable content previews.

Set Up Salesforce CRM Content

USER PERMISSIONS		EDITIONS
To create, edit, or delete library permissions:	Manage Content Permissions OR Manage Salesforce CRM Content	Available in: both Salesforce Classic (not available in all orgs) and Lightning Experience
To create, edit, or delete page layouts and record types:	Manage record types and layouts for Files OR Manage Salesforce CRM Content	Available in: **Essentials**, **Contact Manager**, **Group**, **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions
To create content fields:	Manage Content Properties OR Manage Salesforce CRM Content	
To create libraries:	Create Libraries OR Manage Salesforce CRM Content	
To edit or delete libraries:	Manage Salesforce CRM Content	

Set up Salesforce CRM Content in your org to enable content libraries and set up permissions.

1. From Setup, enter `Salesforce CRM Content` in the `Quick Find` box, select **Salesforce CRM Content**, and then select `Enable Salesforce CRM Content`.

2. Give users access to Salesforce CRM Content by assigning feature licenses in one of the following ways:

   - To assign feature licenses to users automatically, from Setup, enter `Salesforce CRM Content` in the `Quick Find` box, select **Salesforce CRM Content**, and then select `Autoassign feature licenses to existing and new users`.

   - To assign feature licenses to users manually, from Setup, enter `Users` in the `Quick Find` box, then select **Users** and click **Edit** next to the user's name. Select the `Salesforce CRM Content User` checkbox and click **Save**.

3. Verify that the Salesforce CRM Content users have the Salesforce CRM Content user permissions enabled. The user permissions include Manage Salesforce CRM Content, Create Libraries, Manage Content Permissions, Manage Content Properties, Manage record types and layouts for Files, and Deliver Uploaded Files and Personal Content. To add library items as email attachments, a user needs to be a member of the library.

   > **Note:** Users with the Deliver Uploaded Files and Personal Content user permission can create content deliveries from personal libraries. This user permission doesn't affect the ability to deliver content from shared libraries.

4. Use the New Library Wizard to create a library, add members to the library, and assign library permissions to the members.

   > **Note:** You can control access to libraries with library permissions, the groups of privileges that determine user access within a library. Users must be assigned library permissions before they can use libraries. All new organizations contain three library permissions: library administrator, author, and viewer.

5. Categorize and define your content:

a. Create content fields and assign them to page layouts. The default fields are `Description`, `Tags`, and `Title`. If you want to create a field named, for example, `Reviewed By`, your custom content field would be a picklist with the names of possible reviewers.

b. Create a custom page layout or modify the default page layout. Page layouts are the containers for custom fields; they determine which fields are available during the publishing process and how the fields display on the content details page. You can create multiple page layouts and record types and assign a content field to any or all page layouts. For example, if sales and marketing users want to record different information about their content, you can create Sales and Marketing page layouts and record types. If you create a `Related Campaign` lookup field and add it to the Marketing page layout and record type only, users who select the Sales record type during the upload process don't get to choose a campaign.

Implementation Tips

- Before you create libraries, review the files you plan to store to determine how many libraries you need and what content belongs in each library. Users are given access to content based on library.

- If you have a lot of Salesforce CRM Content users, create a public group and add the group to a library rather than adding users to the library individually.

- To enable Salesforce CRM Content functionality for leads, accounts, contacts, opportunities, cases, products, or custom objects, add the Related Content related list to the appropriate page layout.

- To send web-formatted content to colleagues, leads, or contacts and associate it with Salesforce records, add the Content Deliveries related list to the page layout for leads, accounts, contacts, opportunities, cases, campaigns, or custom objects.

- To allow users to publish, edit, and search in any of the Salesforce-supported languages, from Setup, enter `Salesforce CRM Content` in the `Quick Find` box, select **Salesforce CRM Content**, and then click **Enable multilanguage search and contribute**.

- Salesforce CRM Content is available via the Customer Portal and partner portal.

- All Salesforce CRM Content items display as primary tabs in the Salesforce Console.

Best Practices

- If you are using the Related Content related list on Salesforce objects, align your custom content fields with the standard and custom fields on the object to increase the accuracy of a search. Clicking the **Find Content** button on the related list matches content to the fields on the record and displays search results containing the related content.

- To ensure that content is classified consistently, define consistent tag names with your contributors. For example, establish tag names at the outset to avoid having tags such as "channel" and "channels" in the same library.

- Avoid using too many tags. The search engine helps users find specific content, whereas tags enable users to browse and subscribe. Excessive tagging creates unnecessary clutter.

- You can't change or delete tag names. You can remove tags from a document, but that doesn't delete the tag.

- Tags are case insensitive. You can't have two tags with the same name even if they use different upper and lowercase letters. The case of the original tag is always used.

- To highlight valuable content and make it easier to find, mark it as "featured" on the content details page. Featured content receives a higher priority than similar content in search results, and appears on the Libraries tab for easy access. To feature content, users must have the `Feature Content` option checked in their library permission.

- If your organization uses Google Docs, encourage library members to add their Google docs to a library. Including Google docs in Salesforce CRM Content allows users to access all types of content from a single location and apply Salesforce CRM Content functionality, such as votes, comments, and subscriptions, to Google docs.

Tip: For more detailed information about setting up Salesforce CRM Content, refer to the Salesforce CRM Content Implementation Guide.

Salesforce CRM Content is only available in Salesforce Classic, but files from content libraries are available in Lightning Experience if Salesforce CRM Content is enabled for your org.

SEE ALSO:

Customize Salesforce CRM Content

Set Up Content Deliveries

Customize Salesforce CRM Content

Modify content fields, validation rules, library permissions, and other default settings.

From Setup, enter `Salesforce CRM Content` in the `Quick Find` box, and select **Salesforce CRM Content** to access the following options for customizing Salesforce CRM Content:

Tip: To perform the initial setup of Salesforce CRM Content for your organization, see Set Up Salesforce CRM Content on page 78.

- **Content Fields**—Create, edit, or delete custom content fields. Custom fields allow users to categorize and define content during the publishing process.

- **Validation Rules**—Create, edit, or delete validation rules. Validation rules verify that the data a user enters when publishing content meets the standards you specify before the user can save the content.

- **Library Permissions**—Create, edit, or delete library permissions. A library permission determines user privileges within a library.

- **Settings**—Modify Salesforce CRM Content default settings for multi-language support, PDF downloads, content pack creation, or the enhanced document viewer.

SEE ALSO:

Set Up Salesforce CRM Content

EDITIONS

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

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

USER PERMISSIONS

To create, edit, or delete content fields:
- Manage Content Properties

  OR

  Manage Salesforce CRM Content

To define or change field validation rules:
- Customize Application

To create, edit, or delete library permissions:
- Manage Content Permissions

  OR

  Manage Salesforce CRM Content

Modify content settings:
- Manage Salesforce CRM Content

Customize Content Fields

Create, modify, and delete Salesforce CRM Content custom fields so you can categorize and define your content.

To create, modify, and delete Salesforce CRM Content custom fields for categorizing and defining your content, go to the object management settings for content. If you're using Lightning Experience, go to the Object Manager, select **Content Version**, then scroll to the fields area. If you're using Salesforce Classic, enter `Salesforce Files` in the `Quick Find` box, then select **Fields**. The data assigned to these fields during upload is available on the content details page for the life of the file. After creating custom content fields, you must assign them to a page layout. The page layout determines which fields appear when a user uploads or revises files in Salesforce CRM Content.

1. Click **New**.

2. Choose the type of field to create, and click **Next**.

3. For relationship fields, associate an object with the field and click **Next**.

4. Enter a field label. The field name is automatically populated based on the field 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. Ensure the custom field name is not identical to any standard field name for that object.

5. Choose the page layout that should display the field as an editable field.

Click **Edit** or **Del** in the Content Custom Fields & Relationships related list to edit or delete a custom content field. You can't edit or delete the standard content fields. Deleted custom fields and their data are stored until your org permanently deletes them or 15 days has elapsed, whichever happens first. Until that time, you can restore the field and its data.

SEE ALSO:

Customize Salesforce CRM Content

Libraries

Store, share, and manage your files in content libraries.

Create Libraries

Store, share, and manage your files in content libraries so you can decide who has access to files in each library and what permissions they have. Each org can have up to 2,000 libraries.

Manage Library Permissions

A library permission is a group of privileges assigned to each Salesforce CRM Content library member. It determines the tasks that a member can perform in a particular library. The same user can have a different library permission in each library.

Create and Edit Library Permissions

Library permissions provide the different levels of library access that are required for most organizations. Here's how to add new permissions and edit existing ones.

Assign Library Tagging Rules

In Salesforce CRM Content, tags are descriptive labels that help classify and organize content. Contributors can assign tags to their files, Google docs, or web links, to enable all library members to browse for content by tag. The tagging rule in a library determines how contributors can tag content; for example, the restricted-tagging rule does not allow contributors to create tags. Library tagging rules are optional. By default, library contributors can enter any tag.

Restrict Record Types in a Library

Library administrators can choose which record types are available in a library. They can also set the default record type for publishing content to the library.

Set Up Libraries

Libraries are a wonderful way to organize files and manage user permissions. See files displayed in a grid or switch to the familiar list view. Click a library or folder to see files displayed as thumbnails. A thumbnail view is an easy way to find files. With the Libraries component, you can sort files and pinpoint exactly what you're looking for in no time at all.

Create Libraries

Store, share, and manage your files in content libraries so you can decide who has access to files in each library and what permissions they have. Each org can have up to 2,000 libraries.

Step 1: Create a New Library

1. From the My Libraries section of the Libraries tab home page, click **New**.
2. Enter a unique library name.
3. If you want, add a description.
4. Click **Save and Add Members**.

   📝 **Note:** If you want to add members later, click the **Save and Close** button.

Step 2: Add Library Members

1. On the **Libraries** tab, click the library name if the library isn't already open.
2. In the **Members** section, click **Add Members**.
3. If the member you want to add isn't listed, type their first name in the search box and click **Find**.
4. Select members from the Available Members box. Members can include individual Salesforce CRM Content users or public groups containing Salesforce CRM Content users.

   💡 **Tip:** If you have many Salesforce CRM Content users, create a public group and add it to a library rather than adding users to the library individually.

5. To add the members to the library, click **Add**.
6. Click **Next**.

Step 3: Assign Library Permissions to Members

- Select a library permission for each user or public group and click **Save**.

For more information, see Manage Library Permissions on page 84.

📝 **Note:** Libraries are available to users even if they don't have Salesforce CRM Content licenses. In Lightning Experience, users without Content licenses can view libraries and work with library files and folders. In Salesforce Classic, they can view libraries and access files from libraries. Libraries are available without Content by default. Manage these settings in two places:

- To enable access for everyone in your org, go to Setup. Enter *General Settings* in the Quick Find box, then select **General Settings**. Select **Libraries in Salesforce Files**.
- To control access for a subset of users, use the Access Libraries permission, available for profiles and permission sets on most standard user licenses.

Manage Library Permissions

A library permission is a group of privileges assigned to each Salesforce CRM Content library member. It determines the tasks that a member can perform in a particular library. The same user can have a different library permission in each library.

- From Setup, enter `Content Permissions` in the `Quick Find` box, then select **Content Permissions**.
- Next to the appropriate permission, select **Edit** or **Delete**.

📝 **Note:** If your Salesforce CRM Content organization was created after the Spring '09 release, your organization already has three library permissions: Library Administrator, Author, and Viewer. Library permissions don't apply to personal libraries. All Salesforce CRM Content users can save files in their personal libraries.

SEE ALSO:

Create Libraries

Create and Edit Library Permissions

EDITIONS

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

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

USER PERMISSIONS

To create, edit, or delete library permissions:
- Manage Salesforce CRM Content

  OR

  Manage Content Permissions

Create and Edit Library Permissions

Library permissions provide the different levels of library access that are required for most organizations. Here's how to add new permissions and edit existing ones.

To create or edit library permissions in Salesforce CRM Content, from Setup, enter `Content Permissions` in the `Quick Find` box, and select **Content Permissions**. Choose **Add Library Permissions** or **Edit** next to the permission.

💡 **Tip:** If your Salesforce CRM Content organization was created after the Spring '09 release, your organization already has Viewer, Author, and Library Administrator library permissions. If not, consider creating them. For the Viewer library permission, select the `View Comments` and `Add Comments` library privileges. For the Author library permission, select the `Add Content`, `Add Content on Behalf of Others`, `Archive Content`, `Add Comment`, and `Tag Content` library privileges. For the Library Administrator permission, select the `Manage Library` privilege.

1. Assign a name to the library permission.
2. Optionally, enter a description of the library permission. If your organization has several library permissions, consider describing each by its function or with a summary of its privileges.
3. In the Permissions section, select the checkboxes that correspond to the privileges you want to grant to users with this library permission, and click **Save**.

EDITIONS

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

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

USER PERMISSIONS

To create or edit library permissions:
- Manage Salesforce CRM Content

  OR

  Manage Content Permissions

Library Privilege	Description
Manage Library	Perform any action in the library. This privilege is required to edit a library's name and description, add or remove library members, or delete a library. Manage Library is a super permission which provides all the following permission options listed except `Deliver Content.` Creating a library requires the Manage Salesforce CRM Content app permission or Create Libraries system permission.
Add Content	Publish new content to the library, upload new content versions, or restore archived (deleted) content. Content authors can also change any tags associated with their content and archive or delete their own content.
Add Content on Behalf of Others	Choose an author when publishing content in the library.
Archive Content	Archive and restore any content in the library.
Delete Content	Delete any content in the library. Authors can undelete their own content from the Recycle Bin.
Feature Content	Identify any content in the library as *featured*.
View Comments	Read comments posted to any content in the library.
Add Comments	Post comments to any content in the library and view all comments in the library. Users can edit or delete their own comments.
Modify Comments	Edit or delete comments made to any content in the library.
Tag Content	Add tags when publishing content or editing content details in the library.
Deliver Content	Create a content delivery using any files in the library.
Attach or Share Content	Make content from this library accessible in Chatter. Within Chatter, select a file from the library and attach it to a post or share it.
Organize File and Content Folder	Create, rename, and delete folders in libraries in Lightning Experience.

4. Click **Save**.

SEE ALSO:

Create Libraries

Manage Library Permissions

Assign Library Tagging Rules

In Salesforce CRM Content, tags are descriptive labels that help classify and organize content. Contributors can assign tags to their files, Google docs, or web links, to enable all library members to browse for content by tag. The tagging rule in a library determines how contributors can tag content; for example, the restricted-tagging rule does not allow contributors to create tags. Library tagging rules are optional. By default, library contributors can enter any tag.

To assign a tagging rule to a library:

1. On the Libraries tab, select a library from the **My Libraries** area.

2. Click **Tagging Rules** and choose one of the following options:

Library Tagging Rule	Description
Open Tagging	This rule places no restrictions on tagging. Contributors can enter any tag when publishing or editing content. While a tag is typed, Salesforce CRM Content autosuggests tags based on the contributor's recently used tags and the Popular Tags list.
Guided Tagging	This rule also enables contributors to enter any tag when publishing or editing content, but contributors are also offered a list of suggested tags. If you select Guided Tagging, the next step prompts you to enter the suggested tags that you want to recommend to library contributors.
Restricted Tagging	This rule requires contributors to choose from the list of suggested tags. If you select Restricted Tagging, the next step prompts you to enter the list of suggested tags.

3. If you chose **Guided Tagging** or **Restricted Tagging**, click the link for auto-populating the Suggested Tags field and then edit, add, or remove tags as needed. If you do not auto-populate the Suggested Tags field, any new tags you enter in the field are added to the existing list of suggested tags in the library.

4. Click **Save**.

Notes on Library Tagging Rules

- Open Tagging is the default tagging rule.

- If you publish, share, or move content to a library that uses restricted tags, you receive an error if your content contains unsupported tags.

- When you share content from one library to another, the most restrictive tagging rule applies. For example:

  - When content is shared between a restricted-tagging library and a guided- or restricted-tagging library, you can only choose tags that are common to both libraries.

  - When content is shared between an open tagging library and a restricted-tagging library, you can only choose tags suggested in the restricted-tagging library.

- If a restricted tagging rule is applied after content has already been published in the library and the existing content contains tags that are no longer permitted by the rule, the tags remain assigned to the content until it is edited or revised. For example, if the Q3Forecast document has a *market indicators* tag and *market indicators* is not a suggested tag according to the new restricted-tagging rule, *market indicators* is removed from Q3Forecast only when a user publishes a new version of the file or edits the file's tags on the content details page.

- Don't use too many tags. The search engine helps users find specific content. Tags enable users to browse and subscribe. Excessive tagging creates unnecessary clutter.

- You can't change or delete tag names. You can remove tags from a document, but that doesn't delete the tag.

- Tags are case insensitive. You can't have two tags with the same name even if they use different upper and lowercase letters. The case of the original tag is always used.

SEE ALSO:
   Create Libraries

Restrict Record Types in a Library

Library administrators can choose which record types are available in a library. They can also set the default record type for publishing content to the library.

To restrict the record types allowed in a library:

1. On the Libraries tab, select a library from the **My Libraries** area.

2. Click **Record Types**.

3. Optionally, change the default record type for the library.

4. Select the `Restrict the record types available in the library` checkbox.

5. Select one or both of the following options:

   - `Allow content with any record type to be linked to this library`— Select this option if you want to enable content published in other libraries to be shared to the library where you have restricted record types. The content in other libraries can be shared regardless of the record types used.

   - `Do not apply record type restrictions to existing content`— Select this option if you don't want to receive warnings regarding existing content in the library. You won't be alerted if existing content uses record types that you exclude from the library. This option refers to notifications only; existing content is not affected by restricted record types.

6. For each record type that you want to allow in the library, move it from the Available Record Types list to the Selected Record Types list, and click **Save**.

Notes on Restricting Record Types

- If the library already contains published content, selecting the `Restrict the record types available in the library` option automatically moves all the record types used by the published content to the Selected Record Types list.

- Deselecting the `Restrict the record types available in the library` option automatically moves any record types in the Selected Record Types list to the Available record Types list.

- When changing a file's managing library, the file's record type must be permitted in the new managing library.
- When sharing a file with a library, the file's record type must be permitted in the shared library unless the `Allow content with any record type to be linked to this library` option is selected for the shared library.
- When the default record type for a user's profile differs from the default record type for a library, the user profile default takes priority when a user with that profile shares a file with the library. *General* is used as the default record type when no default is set for the user profile.
- When there are no record types in common between a user profile and a library, the default record type for a library is available to users with that user profile who are sharing files with the library.

Set Up Libraries

Libraries are a wonderful way to organize files and manage user permissions. See files displayed in a grid or switch to the familiar list view. Click a library or folder to see files displayed as thumbnails. A thumbnail view is an easy way to find files. With the Libraries component, you can sort files and pinpoint exactly what you're looking for in no time at all.

> **Note:** To use a guided setup, go to **Experience Workspaces** > **Guided Setup**, and select **Intelligent Sales Enablement**. Click **Guided Setup**.

Enable the Library Component
Set up libraries to upload, share, and manage files. You need Salesforce administrator permissions to enable the Libraries component.

Add Library Members
You can add members to libraries. Permissions are customizable from the library level, which gives you control over who can access files.

Create Library Folders
Creating folders gives you more control over the content in your libraries. You can organize folders and subfolders in a way that makes sense to you.

Add Files to a Library
After you have your folder structure set up, you can add files to your folders.

Enable Content Deliveries and Public Links
Use Content deliveries and public links to send links to files to people inside or outside your organization.

Manage Libraries from Files Home
Working in libraries is simpler now that admins can change libraries in Lightning Experience and manage libraries from Files Home.

Manage Library Membership from Files Home
Library admins can update, add, delete, and track library members from Files Home. In the Current Members section, external users automatically get an "external badge" to help you identify external partners, customer site members, and portal and Chatter users.

Customize Experience Builder Site Libraries with Images
Give each library a unique look by branding it with an image.

Enable the Library Component

Set up libraries to upload, share, and manage files. You need Salesforce administrator permissions to enable the Libraries component.

1. Go to **Libraries**, and select **My Libraries**, and click **New**.

    You can give your library a unique name and description in the New Library Wizard.

Add Library Members

You can add members to libraries. Permissions are customizable from the library level, which gives you control over who can access files.

1. Go to **Files**, select **My Libraries**, and click the down arrow on the right side of the library.
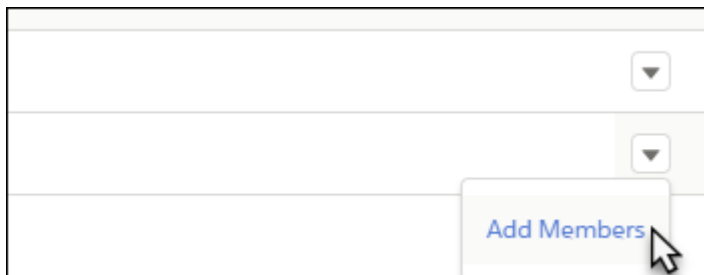
Create Library Folders

Creating folders gives you more control over the content in your libraries. You can organize folders and subfolders in a way that makes sense to you.

1. Go to **Files**, **Libraries**, **Owned By Me**, and click **New Folder**.

    Permissions are assigned at the library level, making your folder structure a great way to manage who can work with files.

Add Files to a Library

After you have your folder structure set up, you can add files to your folders.

1. Go to **Files**, **Libraries**, and click **Add Files**.

Enable Content Deliveries and Public Links

Use Content deliveries and public links to send links to files to people inside or outside your organization.

With content deliveries, you can set a password or an expiration date for the link, and track how frequently the content is viewed. When you create a public link to a file, you can set a password and expiration date. Public links to folders don't have password protection or link expiration. You can't track content views on public links to files or folders.

Any time confidential documents are shared, we recommend requiring password protection.

Other Permissions

In addition to the global settings that enable content deliveries and public links for your org, you need to enable the user permissions "Create Content Deliveries" or "Create Public Links" on profiles or in permission sets.

Files in libraries are governed by settings in the library, not user permissions. To share files managed by a library, Deliver Content must be enabled for the user in the library.

After enabling content delivery and choosing a default for password protection, add the Content Deliveries related list to your page layouts to create new content deliveries and find details about existing deliveries on a record.

1. From Setup, enter `Content Deliveries and Public Links` in the `Quick Find` box, and select **Content Deliveries and Public Links**. Select `Content Deliveries feature can be enabled for users` and `Public Links can be enabled for users (Requires Content Deliveries)`.

2. From Setup, enter `Permission Sets` in the `Quick Find` box, and select **Permission Sets**. Select a permission set, click **System Permissions**, and select `Create Public Links`.

3. From Setup, enter `Profiles` in the `Quick Find` box, and select **Profiles**. Select a profile, and click **Edit**. In **General User Permissions**, select `Create Public Links`. You don't need this permission for files in a shared Salesforce CRM Content library. Instead, complete steps 1 and 2 and then ensure that the user is a library member and that **Deliver Content** is checked in the library permission definition.

4. From Setup, enter `Content Permissions` in the `Quick Find` box, and select **Content Permissions**. Next to Library Administrator in the list of library permissions, click **Edit**, enable **Deliver Content**, and save your changes.

Manage Libraries from Files Home

Working in libraries is simpler now that admins can change libraries in Lightning Experience and manage libraries from Files Home.

Every library that you create is automatically structured in a folder. Library creators have administrator permissions so that they can keep libraries current and relevant.

Start in Files Home. You can sort the order of libraries to work more efficiently. Library users can switch between tile view and list view, and edit libraries in the view that they prefer.

- To create a library and brand your library with a library image, click **New Library**.
- To edit a library, click the dropdown menu next to a library and choose **Edit Library Details**.
- To delete a library, click **Delete**.

    📝 Note: Only empty libraries can be deleted. Delete files first, and then delete the library. If you delete the files and still have trouble deleting the library, permanently delete the files from your Recycle Bin.

EDITIONS

Available in: Lightning Experience

Available in: **Professional**, **Enterprise**, **Performance**, and **Unlimited** Editions
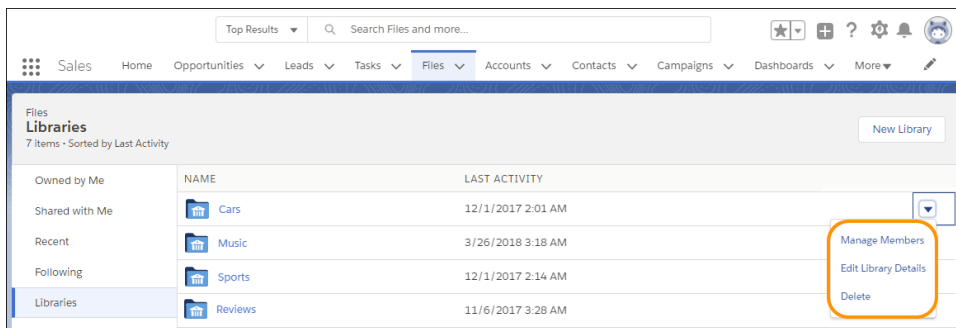
USER PERMISSIONS

To manage a library:
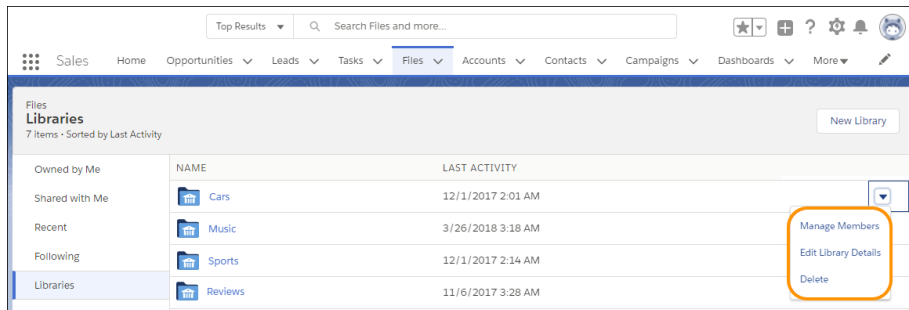- Manage Salesforce CRM Content

    OR

    `Manage Library` checked in your library permission definition

Manage Library Membership from Files Home

Library admins can update, add, delete, and track library members from Files Home. In the Current Members section, external users automatically get an "external badge" to help you identify external partners, customer site members, and portal and Chatter users.

1. To change a library, from Files Home, click **Libraries**.

2. Click the dropdown menu next to a library and choose **Manage Members**.

From here, you can manage members: add them, delete them, or change their permissions.

Customize Experience Builder Site Libraries with Images

Give each library a unique look by branding it with an image.

Library users can identify libraries at a glance without having to figure out which library to access. Library administrators can change images as libraries evolve or switch off branding for their sites.

1. To add a custom library image, from Files Home, click the dropdown to the right of a library, and choose **Edit Library Details**.
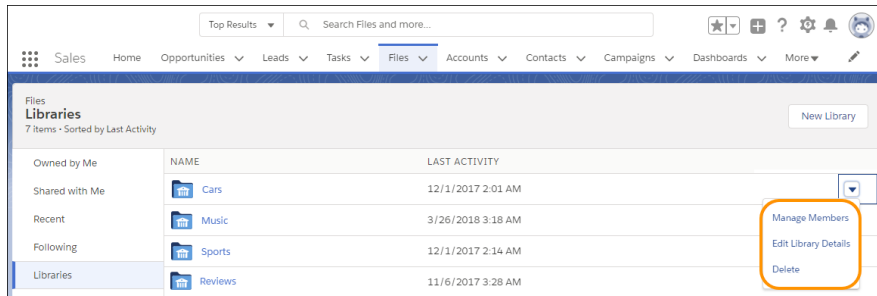
2. Click the **Upload Image** button under Library Image. For best results, choose an image in a 16:9 aspect ratio (for example, 480 pixels by 270 pixels).

> ✏️ **Note:** Branded library images are visible only in the desktop Libraries component tile view. Depending on their permissions, some external users can see library asset images, even if they're not library members. Choose images that you'd like everyone to see. You can remove custom images anytime. If you don't add a custom image, the default library image appears on the folder.

Content Settings

Customize content settings and enable content previews.

Customize Content Settings

Modify the defaults for your Salesforce CRM Content organization and control settings like feature licenses, multilanguage search, and enhanced document viewer.

Allow Content Previews in Link Posts

Salesforce provides rich media support for over 400 URL domains. When you share a supported link in a post, it's converted into embedded videos, images, and other types of previews.

Set Up Content Deliveries

A *content delivery* allows you to convert documents such as Microsoft® PowerPoint and Word files into an optimized web-based version for easy online viewing. After you create your delivery, you can send its encrypted URL to any recipient, such as leads, customers, partners, and colleagues, and then track how often people view or download the content. Content deliveries are available in Salesforce Classic only. However, Lightning Email generates delivery-based links as email attachments for Lightning Experience users who have access to the Content Deliveries feature.

Content Delivery Fields

This table provides a description of the fields that make up a content delivery. These fields are on the create-delivery wizard, the Content Deliveries related list, or the delivery details page.

Customize Content Settings

Modify the defaults for your Salesforce CRM Content organization and control settings like feature licenses, multilanguage search, and enhanced document viewer.

From Setup, enter `Salesforce CRM Content` in the `Quick Find` box, then select **Salesforce CRM Content**.

You can modify the following defaults for your Salesforce CRM Content organization:

Enable Salesforce CRM Content

If this option is checked, Salesforce CRM Content is enabled for your organization.

Autoassign feature licenses to existing and new users

If this option is checked, Salesforce automatically attempts to assign Salesforce CRM Content feature licenses to all existing users. If there aren't enough licenses available, no licenses are assigned. Contact Salesforce to request more feature licenses. When a new user is created, a Salesforce CRM Content feature license is automatically assigned as long as licenses are available. A feature license corresponds to the `Salesforce CRM Content User` checkbox on the user detail page.

Enable multilanguage search and contribute

If this option is checked, a `Language` dropdown list is available when users publish, edit, or search for content. The `Language` dropdown list contains all languages that Salesforce supports. If a user doesn't choose a language when publishing content, that content is associated with the user's personal language by default. If a user's personal language setting is different from the organization's language, content published by that user is associated with the user's language, not the organization's language.

SEE ALSO:

Customize Salesforce CRM Content

Allow Content Previews in Link Posts

Allow Content Previews in Link Posts

Salesforce provides rich media support for over 400 URL domains. When you share a supported link in a post, it's converted into embedded videos, images, and other types of previews.

Enable Chatter before you enable link previews.

1. From Setup, enter `Chatter Settings` in the `Quick Find` box, and select **Chatter Settings**.

2. Click **Edit**, select **Allow Rich Link Previews**, and click **Save**.

Posts that have links to rich media content render those links as previews, like thumbnails, descriptions, and video players. Sometimes a post doesn't render a link as a rich preview in the feed. An unrendered link means the URL domain for that link isn't supported or we weren't able to return the preview for the URL. To generate video previews, your URL must refer to a page that includes metadata for your video in either OpenGraph or oEmbed tags.

Rich media previews are enabled by default. If you disable rich media previews, users can preview only videos from YouTube.

> **Note:** For a look-up list of supported URL domains, see "URL Domains for Rich Link Previews in Feeds."

SEE ALSO:

Customize Content Settings

Set Up Content Deliveries

A *content delivery* allows you to convert documents such as Microsoft® PowerPoint and Word files into an optimized web-based version for easy online viewing. After you create your delivery, you can send its encrypted URL to any recipient, such as leads, customers, partners, and colleagues, and then track how often people view or download the content. Content deliveries are available in Salesforce Classic only. However, Lightning Email generates delivery-based links as email attachments for Lightning Experience users who have access to the Content Deliveries feature.

Content deliveries are available in Salesforce Classic only. However, Lightning Email generates delivery-based links as email attachments for Lightning Experience users who have access to the Content Deliveries feature. In addition to tracking, content deliveries provide several benefits over sending files as attachments, such as giving you control over how long the delivery is available to viewers and whether a viewer can download a file or only view it online. By default, a content delivery shows the most recent version of the file being delivered.

1. From Setup, enter `content deliveries and public links` in the `Quick Find` box, and select **Content Deliveries and Public Links**.

2. Click **Edit**, and then select `Content Deliveries feature can be enabled for users,` `Public Links can be enabled for users (Requires Content Deliveries),` and `Content Deliveries and Public Links can be enabled to let communities users share files managed by libraries (Requires Content Deliveries).`

3. Choose a default option for content-delivery passwords. Because users can send content-delivery URLs to leads, customers, or any unauthenticated user, Salesforce recommends requiring password protection if your users plan to send confidential documents via content delivery. The options allow you to select an organization-wide default for content-delivery password protection.

- **Password protection is optional and defaults to OFF**—If this option is selected, users can choose to require a password when they create a content delivery, but the `Require Password to Access Content` field on the create-delivery wizard is not selected by default.

- **Password protection is optional and defaults to ON**—If this option is selected, the `Require Password to Access Content` field on the create delivery wizard is selected by default. Users can deselect the option if they don't want to require a password.

- **Password protection is required**—If this option is selected, a password is generated each time a content delivery is created. Users cannot opt out of the password requirement.

  📝 Note:

  - If you choose to require a password, users who create a content delivery receive a password when the delivery is generated; users must send the password and the delivery URL to delivery recipients. Delivery recipients are prompted for the password when they click the content delivery URL.

  - Content delivery passwords display with the content-delivery URL when the delivery is created. You can also access the password on the delivery detail page for the life of the content delivery.

  - Files within libraries are governed by settings within the library, so they require an extra setting, in addition to the user permissions. To let a user share files managed by a library, enable **Deliver Content** for that user in the library.

After content delivery is enabled, users can add the Content Deliveries related list to their page layouts for leads, business accounts, contacts, opportunities, cases, campaigns, or custom objects. All Salesforce CRM Content users will see a **Deliver Content** option on each content details page.

Implementation Tips

- To ensure quality of service, the total number of content-delivery views allowed within a 24-hour period is limited to 50,000 and the amount of bandwidth allocated to content deliveries is limited to 50 GB. If recipients try to view deliveries after rate limit are exceeded, they'll be prompted to try again later. Salesforce may be able to increase rate limits on an exception basis. For more information, contact your sales representative.

- When you create a content delivery, Salesforce copies the original file and creates a new version of that file specifically for online viewing. Note the following information concerning supported file types:

  - Microsoft® Office 97 through Microsoft Office 2007 Word, Excel, and PowerPoint files are supported for online views.

  - Adobe® PDF files are supported for online views, but copy-protected PDFs are not.

  - JPG, BMP, GIF, and PNG are supported for online views.

  - Any document over 25 MB isn't supported for online views.

  You can create a content delivery with any file type, but if the file type isn't supported for online viewing, your recipient can only download the document in its original file format.

- Content deliveries require Adobe Flash version 9.0.115. If recipients don't have Flash installed, they can download it.

- Customer portal and partner portal users can't create content deliveries.

- Only the creator of a content delivery can delete the delivery record or edit details such as the expiration date.

- Each time someone clicks a content delivery's URL, Salesforce records the click as one view and distinguishes between internal and external views. An internal view is a view by a Salesforce user. For example, clicking the delivery URL on the delivery detail page or the View option on the Content Deliveries related list is an internal view. The Content Deliveries related list provides a count of all views for each delivery. To see information about a specific view, open the delivery details page.

  📝 Note: For password-protected content deliveries, a view is recorded each time recipients click the delivery URL regardless of whether they enter the password and view the delivery.

- Salesforce CRM Content users can deliver content from shared libraries or a personal library.

Best Practices

- After creating a content delivery, always preview it before sending the URL to your recipients to ensure that the formatting in the original file displays properly in the online version. For example, colors and non-standard fonts don't always display properly in the preview player. If you aren't happy with the quality of the online version, click **Previous** and choose to make your content available in its original file format or as a PDF file only. Your recipients will be able to download the file, and you can use the delivery detail page to track whether recipients download it

- Animation and timings in PowerPoint files aren't supported in the content delivery's online version. Hyperlinks in all file types are also unsupported.

- If you are a Salesforce CRM Content user and want recipients of your content delivery to always see the latest version of a file rather than the version available on the delivery-creation date, open the delivery detail page and click **Edit**. Select the `Content Delivery Opens Latest Version` checkbox.

- If you select `Notify Me of First View or Download`, you'll receive an email when someone views the content delivery for the first time.

Storage Implications

In Salesforce CRM Content, file storage is consumed when content is published to shared libraries or saved to a private library. Creating content deliveries doesn't have an extra effect on storage limits, but users who frequently upload files to their personal libraries for the purpose of content delivery should consider their organization's file-storage limits. Administrators can use reporting to identify who consumes the most storage and which files are largest.

For non-Salesforce CRM Content users, file storage is consumed each time a content delivery is created. After a file is uploaded to Salesforce, it can't be reused for multiple content deliveries. Users need to upload the file each time they want to create a content library. Deleting a content delivery deletes the source file in Salesforce, and increases file-storage space.

SEE ALSO:

Set Up Salesforce CRM Content

Content Delivery Fields

Content Delivery Fields

This table provides a description of the fields that make up a content delivery. These fields are on the create-delivery wizard, the Content Deliveries related list, or the delivery details page.

Field	Description
`Allow Recipient to View in the Browser`	If checked, the content delivery can be viewed in a custom web page. On the delivery details page, this field is labeled `Allow View in the Browser`.

Field	Description
`Allow Recipient to Download as PDF`	If checked, the content delivery converts Microsoft® Word, Excel, and PowerPoint files into PDF files and gives the recipient the option of downloading the PDF. If the file you upload is not a PDF, Word, Excel, or PowerPoint file, this option doesn't appear in the create-delivery wizard. On the delivery details page, this field is labeled `Allow Download as PDF`.
`Allow Download in Original Format`	If checked, the content delivery allows recipients to download the original file. In the create-delivery wizard, this field is called `Allow Recipient to Download as [file type]` where `[file type]` is the original file's file type, such as .ppt, .pdf, or .doc.
`Author`	For Salesforce CRM Content files, the user who published the file. (Read only)
`Content Delivery Name`	The name assigned to the content delivery. By default, the `Content Delivery Name` includes the file name and the creation date.
`Content Delivery Opens Latest Version`	For Salesforce CRM Content files, this flag indicates that the recipient of a content delivery sees the most current version of a file. For example, if a file is updated between the delivery-creation date and today's date, a recipient who views the delivery today sees the newest version.
`Content Delivery Expires`	A flag that indicates whether access to the content delivery expires on the expiration date. In the create-delivery wizard, this flag corresponds to the checkbox next to the `Remove access to content on` field.
`Created By`	The user who created the content delivery, including creation date and time. (Read only)
`Description`	For Salesforce CRM Content files, the description provided when the file was published. (Read only)
`Expiration Date`	The date when the content delivery can no longer be viewed. In the create-delivery wizard, this is the date entered in the `Remove Access to Content on` field.
`File Downloaded`	A flag that indicates whether a file in the content delivery was downloaded. For example, if a content delivery includes options to view the content in a browser, download the content in its original file format, and download the content as a PDF file, this flag is checked if the recipient downloads the original file or the PDF file. (Read only)
`Internal View`	A flag that indicates whether a Salesforce user viewed the content delivery. A view is considered internal if the user opens the delivery URL from within Salesforce, for example by clicking **View** on the Content Deliveries related list or clicking the delivery URL on the

Field	Description
	delivery detail page. If the user copies the URL and pastes it into a browser, the view is considered external. (Read only)
Last Modified By	The user who last modified the content delivery, including modification date and time. (Read only)
Last Viewed	The date and time on which the content delivery was last viewed. A view is one click of the content-delivery URL. (Read only)
Notify Me of First View or Download	If checked, the user who created the content delivery receives an email notification the first time the content delivery URL is clicked.
Owner Name	The user who owns the content delivery. (Read only)
Related To	The record that the content delivery is associated with, such as an account, opportunity, or custom object. Users with sharing access to the record can click it to view more details.
Require Password to Access Content	If checked, the recipient must enter the provided password before viewing the content delivery. The password appears when the content delivery is generated and for the life of the delivery on the delivery detail page.
Title	For Salesforce CRM Content files, the title of the file included in the content delivery. (Read only)
View Count	Total number of views for the content delivery, including internal and external. (Read only)

SEE ALSO:

Set Up Content Deliveries

Google Apps

Enable Google apps like Google Docs, Gmail, and Google-related AppExchange apps—customized for use within Salesforce.

Get Started with Salesforce and Google Apps

Google Apps is a suite of on-demand communication and collaboration services hosted by Google and designed for business users.

Get Started With Salesforce and Google Apps Supported

The Salesforce and Google Apps Supported feature includes a Google Apps Premier Edition account for your organization. In Salesforce, you can create that account or upgrade from an existing Google Apps Standard Edition account to Google Apps Premier Edition.

Set Up Google Apps in Salesforce

Edit domain settings and modify Google Apps services.

Get Started with Salesforce and Google Apps

Google Apps is a suite of on-demand communication and collaboration services hosted by Google and designed for business users.

📝 **Note:** Not all Google Apps features are available in Lightning Experience. The features that are available may not look the same as they do in Salesforce Classic.

If your organization has a Google Apps account, Salesforce administrators can enable Google Docs, Gmail, and a host of Google-related AppExchange apps—customized for use within Salesforce.

Step 1: Creating a Google Apps Account

Create a Google Apps account for your organization using one of the following methods:

- From Setup, enter `Google Apps` in the `Quick Find` box, select **Google Apps Settings**, and click **Sign Up** to launch the account-creation page on the Google website. You are prompted to register your organization's domain name or purchase a new domain name from Google. A domain is the portion of a website's URL that follows the "www." Follow Google's steps to configure your new or existing domain and set up your Google Apps account.

- If your organization purchased the Salesforce and Google Apps Supported feature, from Setup, enter `Premier Setup` in the `Quick Find` box, then select **Premier Setup** to create a new Google Apps Premier Edition account or upgrade your existing Standard Edition account to Premier Edition. For details, see Get Started With Salesforce and Google Apps Supported.

📝 **Note:** Google Apps in Salesforce supports Google Apps business accounts but not consumer accounts. You can identify a consumer account by the "gmail.com" domain in an email address; for example, `myname`@gmail.com is a consumer account. The Google Apps domain you set up in Salesforce must be the domain you registered with Google for your organization; for example, `mycompany`.com is a business rather than consumer account.

Step 2: Configuring Google Apps Domain Settings

1. On the Google Apps Settings page in Salesforce, click **Edit**.

2. Choose a user for the `Google Apps Administrative Contact` field. This person is the point of contact for Google Apps users in your organization; specifically, if a user cannot access a Google Apps service, he or she is directed to contact the Google

Apps Administrative Contact. The Google Apps Administrative Contact does not need to be the same person who is registered as your organization's Google Apps administrator with Google, but only the Google Apps administrator can create new Google Apps users on your domain.

3. Enter the `Google Apps Domain` that you registered with Google. For example, if your company's URL is `http://www.acme.com` and you created a Google Apps account for the acme.com domain, enter *acme.com* in the `Google Apps Domain` field.

4. Click **Save**.

Step 3: Activating Google Apps Services

1. In the Activate Google Apps Services section on the Google Apps Settings page, locate the Google Apps service(s) that you want to activate.

2. Click **Edit** or **Install** to activate a service. In the Action column, **Edit** corresponds to Google Apps services that are already integrated in Salesforce, and **Install** corresponds to uninstalled Salesforce AppExchange apps. Integrated Google Apps services include:

- Add Google Docs to Salesforce
- Gmail to Salesforce
- Gmail Buttons and Links
- Google Talk Sidebar Component

> **Important:** Google Talk within Salesforce is no longer available. For alternative ways to use Google Talk, see the Google Talk online help.

For descriptions of the Google-related AppExchange apps, visit https://appexchange.salesforce.com.

Step 4: Creating Google Apps Users

Activating Google Apps services in Salesforce makes the services visible to all users in your organization, but a user cannot access a service unless he or she has a Google Apps account on your organization's domain. The Google Apps administrator registered with Google can create these additional accounts. For more information, see Create Google Apps Accounts.

SEE ALSO:

Get Started With Salesforce and Google Apps Supported

Set Up Google Apps in Salesforce

Activate Google Docs in Salesforce

Gmail™ in Salesforce

Get Started With Salesforce and Google Apps Supported

The Salesforce and Google Apps Supported feature includes a Google Apps Premier Edition account for your organization. In Salesforce, you can create that account or upgrade from an existing Google Apps Standard Edition account to Google Apps Premier Edition.

After you create a new Google Apps Premier Edition account or upgrade your existing Google Apps Standard Edition account in Salesforce, the Premier Setup page displays your organization's domain name, the number of Google Apps Premier Edition licenses available to your organization, and, if applicable, the status of your upgrade.

Creating a New Google Apps Premier Edition Account

If your organization does not have a Google Apps account, complete the following steps to register a Google Apps Premier Edition account and enable Salesforce and Google Apps:

1. From Setup, enter `Premier Setup` in the `Quick Find` box, then select **Premier Setup**.

2. Complete the fields in Column A:

Field	Description
Domain Name	Enter the domain that you want to register as your organization's Google Apps account. For example, if your company's URL is `http://www.acme.com`, enter `acme.com` as your Domain Name.
User Name	This value is used to create the Google Apps administrator for your organization's account. For example, if your Google Apps administrator will be jsmith@acme.com, enter `jsmith`. After your Google Apps account is created, you can log in with the `User Name` and `Password` and change this value if necessary.
First Name	This value is used to create the Google Apps administrator for your organization's account. After your Google Apps account is created, you can log in with the `User Name` and `Password` and change this value if necessary.
Last Name	This value is used to create the Google Apps administrator for your organization's account. After your Google Apps account is created, you can log in with the `User Name` and `Password` and change this value if necessary.
Email Address	This email address receives a confirmation notice when your Google Apps Premier

Field	Description
	Edition account is created. Google does not store this value for any other purpose.
Password	The Google Apps administrator can log in to Google Apps with this password.
Confirm Password	The Google Apps administrator can log in to Google Apps with this password.

3. Click **Create New Premier Account**.

4. To enable Salesforce and Google Apps, from Setup, enter `Google Apps Settings` in the `Quick Find` box, then select **Google Apps Settings**.

5. Choose a user for the `Google Apps Administrative Contact` field. This person is the point of contact for Google Apps users in your organization; specifically, if a user cannot access a Google Apps service, he or she is directed to contact the Google Apps Administrative Contact. The Google Apps Administrative Contact does not need to be the same person who is registered as your organization's Google Apps administrator with Google, but only the Google Apps administrator can create new Google Apps users on your domain.

6. Verify that the `Google Apps Domain` field contains the domain name you registered with Google.

7. Activate Google Apps services in Salesforce. For more information, see Activating Google Apps Services.

8. Create users for your organization's Google Apps account. For more information, see Create Google Apps Accounts.

> 📝 Note: The number of Google Apps Premier Edition accounts you can create is limited to the number of licenses your organization purchased with the Salesforce and Google Apps Supported feature.

Upgrading to a Google Apps Premier Edition Account

Complete the following steps to upgrade your organization's existing Google Apps Standard Edition account to a Google Apps Premier Edition account.

1. From Setup, enter `Premier Setup` in the `Quick Find` box, then select **Premier Setup**.

2. Complete the fields in Column B:

Field	Description
Domain Name	The domain that you want to register as your organization's Google Apps Premier Edition account. If you already enabled Salesforce and Google Apps, this field is prepopulated with your organization's domain name.
Google Apps Token	The 16-digit token required to upgrade from Google Apps Standard Edition to Google Apps Premier Edition. Your organization's Google Apps administrator can access this information on the Google website. For more information, click **Retrieve Google Apps Token** in Column B.

3. Click **Upgrade Existing Account to Premier**.

4. To enable Salesforce and Google Apps, from Setup, enter `Google Apps Settings` in the `Quick Find` box, then select **Google Apps Settings**.

5. As needed, edit the `Google Apps Administrative Contact` field. This person is the point of contact for Google Apps users in your organization; specifically, if a user cannot access a Google Apps service, he or she is directed to contact the Google Apps Administrative Contact. The Google Apps Administrative Contact does not need to be the same person who is registered as your organization's Google Apps administrator with Google, but only the Google Apps administrator can create new Google Apps users on your domain.

6. Verify that the `Google Apps Domain` field contains the domain name you registered with Google.

7. As necessary, activate Google Apps services in Salesforce. For more information, see Activating Google Apps Services.

8. As necessary, create users for your organization's Google Apps account. For more information, see Create Google Apps Accounts.

> Note: The number of Google Apps Premier Edition accounts you can create is limited to the number of licenses your organization purchased with the Salesforce and Google Apps Supported feature.

SEE ALSO:

Get Started with Salesforce and Google Apps

Set Up Google Apps in Salesforce

Edit domain settings and modify Google Apps services.

> Note: Not all Google Apps features are available in Lightning Experience. Those that are available may not look the same as they do in Salesforce Classic.

From Setup, enter `Google Apps Settings` in the `Quick Find` box, then select **Google Apps Settings** to edit your Google Apps domain settings, activate or deactivate Google Apps services in Salesforce, or install or uninstall Google-related Salesforce AppExchange packages..

> Important: You cannot use Salesforce and Google Apps until a Google Apps account has been created for your organization and your Google Apps domain settings are configured in Salesforce. For instructions on creating an account and configuring your domain settings, see Get Started with Salesforce and Google Apps on page 101.

Editing Google Apps Domain Settings

Domain settings consist of two values: the user chosen to administer your organization's Google Apps account and the domain your organization registered with Google. Both fields are required to enable Google Apps in Salesforce. To edit your domain settings:

1. In the Configure Google Apps Domain section, click **Edit**.

2. Optionally, choose a new user for the `Google Apps Administrative Contact` field. This person is the point of contact for Google Apps users in your organization; specifically, if a user cannot access a Google Apps service, he or she is directed to contact the Google Apps Administrative Contact. The Google Apps Administrative Contact does not need to be the same person who is registered as your organization's Google Apps administrator with Google, but only the Google Apps administrator can create new Google Apps users on your domain.

EDITIONS

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

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

USER PERMISSIONS

To edit Google Apps domain settings and activate or deactivate services:
- Customize Application

To install or uninstall AppExchange packages:
- Download AppExchange packages

3. Optionally, modify the `Google Apps Domain` that is registered with Google for your organization's Google Apps account. Your `Google Apps Domain` is typically your company's domain; for example, acme.com.

Modifying Google Apps Services

This section lists Google Apps services that are integrated with Salesforce and also provides links to several Google-related Salesforce AppExchange apps that can be easily installed from AppExchange.

To activate or deactivate an integrated service, click **Edit** next to the service name. These services include:

- Add Google Docs to Salesforce
- Gmail to Salesforce
- Gmail Buttons and Links
- Google Talk Sidebar Component

> 🛑 **Important:** Google Talk within Salesforce is no longer available. For alternative ways to use Google Talk, see the Google Talk online help.

To install or uninstall an AppExchange app, click **Install** or **Uninstall** next to the appropriate name. To view all Google-related AppExchange offerings, visit https://appexchange.salesforce.com.

Implementation Tips

- For detailed information about Google Apps, refer to Google's online help.
- Google Apps in Salesforce is available for Google business accounts but not consumer accounts. You can identify a consumer account by the "gmail.com" domain in an email address; for example, `myname`@gmail.com is a consumer account. The Google Apps domain you set up in Salesforce must be the domain you registered with Google for your organization; for example, `mycompany`.com is a business rather than consumer account.
- After creating a Google Apps account for your organization, create Google Apps accounts for your Salesforce users. From Setup, enter `Users` in the `Quick Find` box, select **Users**, and then click **Export to Google Apps**.
- Notify users of their Google Apps usernames and passwords.
- Notify users about the changes they will see in Salesforce when Google Apps services are activated.
- To view all the Google apps available on Salesforce AppExchange, visit https://appexchange.salesforce.com.
- By default, Google Apps users on your organization's domain can share Google docs with Google Apps accounts outside your domain. The control panel for your Google Apps account contains sharing settings that enable you to restrict document sharing to within your domain.
- When the Add Google Docs to Salesforce service is deactivated, Google docs can't be accessed from Salesforce records. In addition, any Google docs in users' Recycle Bins that were deleted from a record are permanently removed from Salesforce. If the Add Google Docs to Salesforce service is reactivated within 30 days, Google docs that were associated with Salesforce records before the deactivation are restored to their previous location. Deactivating the Add Google Docs to Salesforce service does not affect Google docs in Salesforce CRM Content libraries. Deactivation doesn't remove Google docs associations in libraries and doesn't permanently delete Google docs in Recycle Bins.
- Customer Portal and partner portal users with access to the Contribute tab in Salesforce CRM Content can create new Google docs and associate existing Google docs to a Salesforce library. Portal users without access to Salesforce CRM Content can associate an existing Google doc to a record, but they cannot create new Google docs from within a record because they do not have access to the Google Docs, Notes, and Attachments related list in the portal. Portal users cannot use the **Add Google Doc to Salesforce** browser button.
- Customer Portal and partner portal users cannot access Gmail Buttons and Links.

- If your organization purchased the Salesforce for Google Apps Supported feature, see Get Started With Salesforce and Google Apps Supported on page 103.

Best Practices

- Test your Google Apps integration using a sandbox or Developer Edition organization.

- Manage Google Apps users as you would Salesforce users. For example, if you deactivate a Salesforce user, also deactivate his or her Google Apps account in the control panel for your organization's Google Apps account. For information about administering your organization's Google Apps account, refer to Google's online help.

- To locate a Google doc quickly in Salesforce, search for the doc using search.

SEE ALSO:

Get Started with Salesforce and Google Apps

Create Google Apps Accounts

To access the Google Apps services that are enabled in Salesforce, each user needs a Google Apps account on the domain your organization registered with Google. An account includes a username and password that allow the user to log in to all Google Apps services.

After creating a Google Apps account for your organization and enabling Google Apps in Salesforce, you can create Google Apps accounts for individual users.

> **Note:** If your organization purchased Salesforce and Google Apps Supported, the number of Google Apps Premier Edition accounts you can create is limited to the number of licenses your organization purchased.

1. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.

2. In the View drop-down list, choose a list of users.

3. Click **Export to Google Apps** to export all the users in the list. To export certain users only, select those users in the Action column.

   > **Note:** If Google Apps is not enabled for your organization, the **Export to Google Apps** button does not display. To enable Google Apps in Salesforce, see Get Started with Salesforce and Google Apps on page 101.

4. On the Export Users to Google Apps page, click the export file link that is labeled as Step 1. The name of the link depends on the list view you chose to export; for example, if you were viewing the All Users list, the link on the Export Users to Google Apps page is **All Users Export File**.

5. In the CSV spreadsheet that displays when click you the export link, provide a temporary password for each user. You can modify the `username`, `last name`, and `first name` fields for any user as needed. Google creates account names by adding your domain to the usernames in the spreadsheet; for example, if your domain is acme.com and the spreadsheet contains john.doe and jane.doe usernames, the Google Apps usernames are john.doe@acme.com and jane.doe@acme.com.

6. Save the spreadsheet to your computer.

7. Click the **Google Apps Bulk User Import Tool** link to launch the Bulk Account Update page for your organization's Google Apps account. If prompted, log in with your Google Apps administrator username. Only the user who is registered with Google as the administrator of your organization's account can create additional Google Apps accounts on your organization's domain.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

Export users to Google:
- Customize Application

Create Google Apps accounts:
- Google Apps administrator

8. Follow Google's instructions to import the data in the spreadsheet. The Google Apps administrator receives a confirmation report, and the user for each successfully created account receives a notification email at his or her new Gmail account.

9. Notify users of their usernames and passwords. They will need this information to use any Google Apps service that is enabled in Salesforce.

SEE ALSO:

Get Started with Salesforce and Google Apps

Activate Google Docs in Salesforce

Google Docs™ allows you to create on-demand documents, spreadsheets, and presentations, edit them in your browser, and work together in real time with other collaborators.

> Note: Google Docs appear in Lightning Experience, but they switch to Salesforce Classic when clicked. The Add Google Doc button isn't available in Lightning Experience. Google Apps Settings isn't available in Lightning Experience Setup.

> Important: After you activate a Google Apps service in Salesforce, it's visible to all your Salesforce users. To use these services, your users need Google Apps accounts on your domain. For more information, see Get Started with Salesforce and Google Apps.

To activate or deactivate the Add Google Docs to Salesforce service:

1. In Salesforce Classic Setup, enter `Google Apps Settings` in the `Quick Find` box, then select **Google Apps Settings**.

2. Click **Edit** next to the Add Google Docs to Salesforce option in the Activate Google Apps Services list.

3. Select `Activate`.

4. Read and indicate whether you agree to the Terms of Use.

5. Click **Save**.

When the Add Google Docs to Salesforce service is enabled, these changes allow users to create, edit, or view Google docs and associate them with Salesforce records.

- The Notes & Attachments related list on accounts, assets, contacts, contracts, leads, opportunities, products, and custom objects is renamed to Google Docs, Notes, & Attachments.

- The Attachments related list on cases, solutions, and campaigns is renamed to Google Docs & Attachments.

- If Salesforce CRM Content is enabled, the Libraries tab has an **Add Google Doc** dropdown list.

Users can also install the **Add Google Doc to Salesforce** browser button. The browser button allows them to associate a Google doc to several Salesforce records or a Salesforce CRM Content library without being logged in to Salesforce.

Implementation Tips

- For information about Google Docs, refer to Google's online help.

- By default, Google Docs users on your domain can share their Google docs with Google Apps accounts outside your domain. The control panel in your Google Apps account contains sharing settings that enable you to restrict document sharing to users within your org's domain.

- Customer Portal and partner portal users with access to the Contribute tab in Salesforce CRM Content can create Google docs and associate existing Google docs to a Salesforce library. Portal users without access to Salesforce CRM Content can associate an existing

Google doc to a record, but they cannot create new Google docs from within a record because they do not have access to the Google Docs, Notes, and Attachments related list in the portal. Portal users cannot use the **Add Google Doc to Salesforce** browser button.

- When the Add Google Docs to Salesforce service is deactivated, Google docs can't be accessed from Salesforce records. In addition, any Google docs in users' Recycle Bins that were deleted from a record are permanently removed from Salesforce. If the Add Google Docs to Salesforce service is reactivated within 30 days, Google docs that were associated with Salesforce records before the deactivation are restored to their previous location. Deactivating the Add Google Docs to Salesforce service does not affect Google docs in Salesforce CRM Content libraries. Deactivation doesn't remove Google docs associations in libraries and doesn't permanently delete Google docs in Recycle Bins.

- If Google docs are referenced in Apex, the Add Google Docs to Salesforce service can't be disabled for your org.

- Google docs count against data storage. For each Google doc associated with a record or library in Salesforce, two Kb of storage is used.

SEE ALSO:

Get Started with Salesforce and Google Apps

Gmail™ in Salesforce

Salesforce offers several options to integrate with Gmail. Your options depend on whether you are using Lightning Experience or Salesforce Classic.

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

Gmail Integration Options in Lightning Experience

In Lightning Experience, the following options are available to log emails and use Gmail:

Send Through Gmail

For reps who spend most of their time in Salesforce, but want to use a Gmail account to send emails. Emails are composed in Salesforce, but are sent through a connected Gmail account, and appear in the Gmail Sent Folder. When Send through Gmail is enabled, the Activity History on leads and contacts includes a Compose Gmail button. Emails are logged to the records the email was sent from. See Send Email Through Gmail or Office 365 in Lightning Experience.

Gmail Integration

For reps who spend most of their time in their Gmail account. When emails are sent, reps select which Salesforce records to log the emails to. See Gmail Integration.

Einstein Activity Capture

For users who prefer to have emails logged automatically. Einstein logs email activity from a connected client or device, including Gmail. See Einstein Activity Capture.

Gmail Integration Options in Salesforce Classic

In Salesforce Classic, you can integrate Gmail to Salesforce in the following ways:

- Gmail to Salesforce
- Gmail Buttons and Links

Note: The Gmail integration is also available for Salesforce Classic users. See Gmail Integration.

Gmail to Salesforce

Gmail to Salesforce lets you log emails automatically. It also lets you log chats you send from your Mails account as activities on leads, contacts, opportunities, and other records that support activity history. It's important to know that after you activate Gmail to Salesforce, you can't deactivate it.

To activate Gmail to Salesforce:

1. From Setup, enter `Email to Salesforce` in the `Quick Find` box, then select **Email to Salesforce**. Confirm that it's activated.

2. From Setup, enter `Google Apps Settings` in the `Quick Find` box, then select **Google Apps Settings**.

   > 🛑 **Important:** After you activate a Google Apps service in Salesforce, it's visible to all your Salesforce users. To use these services, your users need Google Apps accounts on your domain. For more information, see Get Started with Salesforce and Google Apps.

3. Set a Google Apps Administrative Contact and Google Apps Domain, then save your changes.

Gmail Buttons and Links

Gmail Buttons and Links adds **Gmail** links next to email fields on all records and adds **Compose Gmail** buttons in Activity History on leads and contacts. When you select a Gmail link or **Compose Gmail**, Salesforce automatically logs you in to your Gmail account and automatically populates the **To** field. If Gmail to Salesforce is activated, Salesforce also populates the **BCC** field with your Email to Salesforce address.

To activate Gmail Buttons and Links:

1. From Setup, enter `Google Apps` in the `Quick Find` box, then select **Google Apps Settings**.

2. In the Activate Google Apps Services list, click **Edit** next to Gmail Buttons and Links.

3. To activate Gmail Buttons and Links, select `Active`.

4. To add **Gmail** links next to all email fields (except email fields on pages under Setup), select `Gmail Links`

5. To add **Compose Gmail** buttons in Activity History on leads and contacts, select `Gmail Buttons`.

6. Read and indicate whether you agree to the Terms of Use.

7. Click **Save**.

Implementation Notes

If you use Gmail Buttons and Links without Gmail to Salesforce, you can still use the Gmail links on contacts and leads. But keep in mind that Salesforce doesn't log emails you send from your Gmail account. Salesforce also doesn't automatically populate the **BCC** field on the **Compose Mail** window with an Email to Salesforce address.

SEE ALSO:

    Get Started with Salesforce and Google Apps

    Google Online Help

Use Google Talk in Salesforce

Google Talk within Salesforce is no longer available. Learn how to deactivate it.

⛔ **Important:** Google Talk within Salesforce is no longer available. For alternative ways to use Google Talk, see the Google Talk online help.

Deactivating Google Talk

To deactivate Google Talk in Salesforce:

1. From Setup, enter `Google Apps` in the `Quick Find` box, then select **Google Apps Settings**.
2. Click **Edit** next to the Google Talk Sidebar Component option in the Activate Google Apps Services list.
3. Deselect the `Active` checkbox.
4. Click **Save**.

SEE ALSO:

> Get Started with Salesforce and Google Apps

Collaboration Resources for Admins

In addition to online help, Salesforce publishes printable documentation to help you learn about our features and successfully administer Salesforce.

	For End Users	For Admins
Collaboration		
Quick Actions Implementation Guide		✔
Set Up Salesforce Files Sync		✔
Salesforce Files Connect Implementation Guide		✔
Experience Cloud		
Set Up and Manage Experience Cloud Sites		✔
Community Management Guide for Experience Cloud		✔
Salesforce CRM Content		
Salesforce CRM Content Implementation Guide	✔	✔

INDEX

S