



Lightning Sync Design and Security

Salesforce, Spring '24

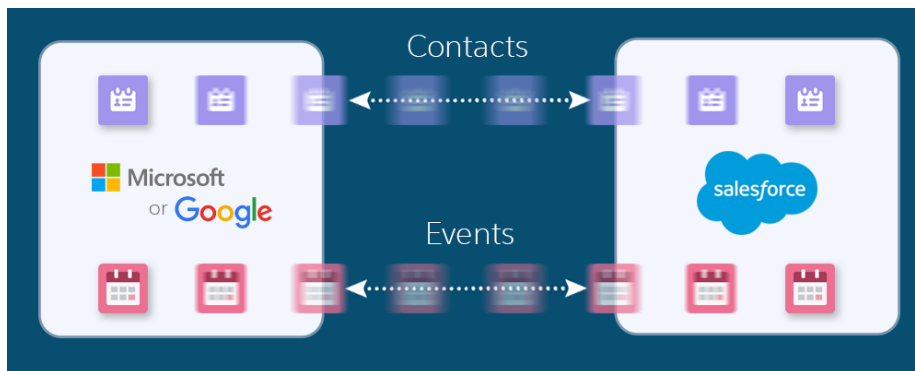


CONTENTS

LIGHTNING SYNC OVERVIEW	1
LIGHTNING SYNC DESIGN AND DATA FLOW	2
LIGHTNING SYNC CONNECTION SECURITY	3
SECURITY MEASURES SPECIFIC TO YOUR CONNECTION METHOD	4
Service Account Connection for Microsoft Users	4
OAuth 2.0 Connection for Microsoft Users	6
Connection for Google G Suite Users	7
LIGHTNING SYNC TRANSACTIONS	9

LIGHTNING SYNC OVERVIEW

Learn about how Lightning Sync is designed to sync contacts and events between your users' Microsoft® Exchange or Google G Suite account and Salesforce. Plus, learn how our design prioritizes the security of your data when it's transferred between systems.



Your users are more productive when their contacts and events sync between your company's email service and Salesforce. Syncing avoids duplicating work between the two systems. Plus, contacts and events sync whether users are working from their desks or from the Salesforce app.

Salesforce admins define the sync experience by selecting users' sync settings in Salesforce. Admins can choose:

- Which users sync
- To sync contacts, events, or both
- Which direction items sync
- To sync all events or only the events users select using the [Outlook Integration](#) or [Google Integration](#) apps
- To sync event series (Exchange and Lightning Experience or Salesforce mobile app only)
- To sync private events
- To automatically relate contacts or one lead to syncing events in Salesforce
- To automatically remove deleted events from the other application

Plus, because Lightning Sync is a cloud-based solution, users get product improvements automatically during the major Salesforce releases. Unlike our legacy sync feature, Salesforce for Outlook, no manual software installation is required.

SEE ALSO:

[Explore Email and Calendar Integration Products](#)

EDITIONS

Available to sync records from: Salesforce Classic, Lightning Experience, and the Salesforce mobile app

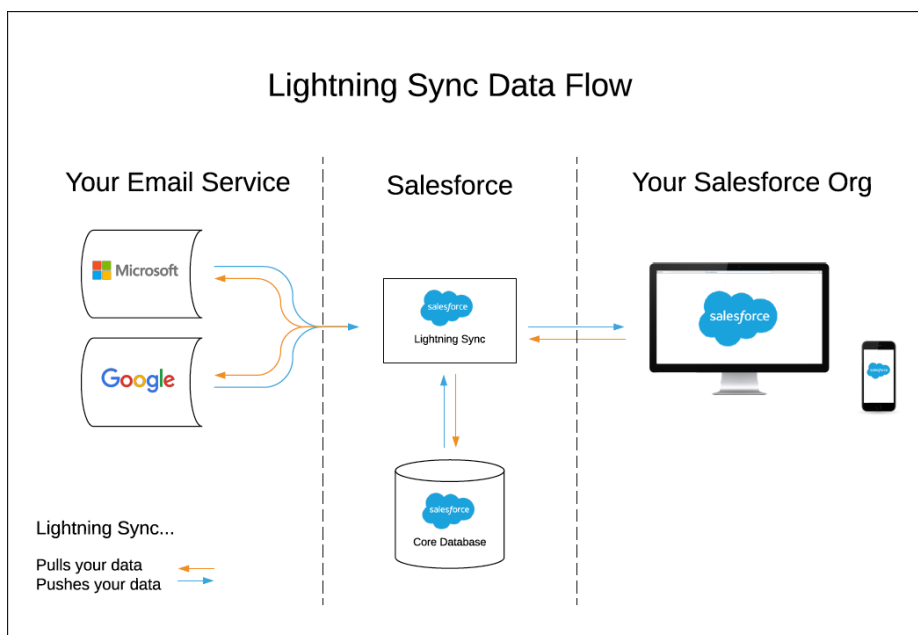
Available to set up from: Salesforce Classic and Lightning Experience

Available in: **Professional, Enterprise, Performance, Unlimited, and Developer** Editions with Sales Cloud, Service Cloud, and Lightning Platform

LIGHTNING SYNC DESIGN AND DATA FLOW

Lightning Sync is designed to simplify the data flow between Salesforce and your email service.

Lightning Sync connects the core Salesforce database with your email server directly, with no email client required to maintain synchronization. This design simplifies the connection process and makes Lightning Sync a superior solution to Salesforce for Outlook, which requires a connection to individual Outlook user accounts. Calls to sync are made from an automated process on the Salesforce core stack to your email service, regardless of which data store has been updated. Users don't directly invoke communication between the systems. Likewise, the email service doesn't initiate communication.



With Lightning Sync, Data is stored in two locations only: users' individual email services and the Salesforce core database.

LIGHTNING SYNC CONNECTION SECURITY

Salesforce takes your data security seriously. Lightning Sync leverages standard Salesforce security measures when establishing a connection with your email service.

Lightning Sync establishes a connection with your email service when you set up the product. When establishing a connection, Salesforce verifies the authenticity of your Microsoft or Google service with a security certificate that meets our certificate standards.

- Microsoft® Office 365® and Google G Suite automatically provide certificates that comply.
- Microsoft Exchange 2019, 2016, and 2013 customers are required to configure a certificate signed by one of the [Salesforce-Approved certificate authorities](#).

After the connection is established, Lightning Sync transfers contact and event data between servers. Individual users aren't required to log in to sync.

To avoid the possibility of interception, Salesforce uses TLS technology to protect transferred data. Upon authorization of each transaction, Salesforce requires the TLS configuration from the data received to meet Salesforce TLS security requirements before granting access.

SEE ALSO:

[Security Infrastructure](#)

SECURITY MEASURES SPECIFIC TO YOUR CONNECTION METHOD

When you prepare your email service to connect with Salesforce, you create touchpoints in which the systems connect to sync data. Lightning Sync provides several methods for connecting systems. The security measures and other benefits that impact you depend on which connection method you select when you set up the product. See which connection methods are available to you based on the email service that you're using. Then learn about the security measures that impact that connection method.

[Service Account Connection for Microsoft Users](#)

The service account connection method is available for Lightning Sync users working on Microsoft® Exchange 2019, 2016, and 2013 and on Microsoft Office 365® (Exchange Online). For Exchange Online customers, the service account connection method is no longer available starting October 1, 2022.

[OAuth 2.0 Connection for Microsoft Users](#)

Connecting with OAuth 2.0 is available for Lightning Sync users working from Microsoft® Office 365®. To learn more, see the Lightning Sync system requirements.

[Connection for Google G Suite Users](#)


The Google G Suite connection method is a combination of an OAuth 2.0 and a service account connection. This design is based on a method recommended by Google for connecting server to server.


SEE ALSO:

[Lightning Sync System Requirements](#)

Service Account Connection for Microsoft Users

The service account connection method is available for Lightning Sync users working on Microsoft® Exchange 2019, 2016, and 2013 and on Microsoft Office 365® (Exchange Online). For Exchange Online customers, the service account connection method is no longer available starting October 1, 2022.

 **Important:** Where possible, we changed noninclusive terms to align with our company value of Equality. We maintained certain terms to avoid any effect on customer implementations.

 **Note:** Microsoft is retiring Basic Authentication for Exchange Online. When Microsoft blocks Basic Authentication in your Microsoft tenant, Lightning Sync can't sync contacts and events for customers who have selected service account as their Lightning Sync connection method. See [Lightning Sync Service Account Connection Method Availability for Customers on Microsoft Office 365](#).

Requirement	Why it's required	Benefit to you
Exchange admins must enable Exchange Web Services (EWS) over a connection using TLS 1.2 or higher.	EWS enabled over a TLS connection provides secure certificate authentication between Exchange and Salesforce. While EWS provides access to more objects in your email service, Lightning Sync can only read, write, and update contacts and events from users' email services. Lightning Sync isn't designed to discover or access other objects.	Lightning Sync was designed following the Microsoft-established best practices for the application of EWS. Lightning Sync uses the Exchange server's certificate to authenticate over a TLS connection, confirming that Exchange isn't

Requirement	Why it's required	Benefit to you
	Learn More	<p>interacting with a Salesforce impostor. You can control the scope by which Lightning Sync has access to your email service. To do so, limit which users are impersonated with your service account.</p> <p>Learn More</p>
Exchange admins must enable Auto Discovery.	<p>Auto Discover lets Lightning Sync navigate to the Exchange service endpoint and identify individual users to sync.</p> <p>Learn More</p>	<p>Lightning Sync can identify all users set to sync from the scope of your service account and your sync configuration in Salesforce. Auto Discovery lets Lightning Sync identify even addresses that are part of a different domain.</p> <p>We limit Lightning Sync access to your email service by exploring only your primary email domain with Auto Discovery, which minimizes opportunities for data interception. You can include more domains to sync by adding them manually on the Lightning Sync Setup page in Salesforce. You can also control access by limiting which email service users are impersonated with your service account.</p> <p>Learn More</p>
Exchange admins must enable Basic Authentication or NTLM on your email server and on your autodiscover server.	<p>Lightning Sync identifies itself to your email services using the authentication protocol you chose to enable on your Exchange server. Lightning Sync authenticates on every connection request Salesforce makes to Exchange. If Basic and NTLM are enabled, Lightning Sync gives connection preference to Basic. If you must run other authentication methods on your server, those methods don't conflict with the Lightning Sync connection.</p> <p>Learn More</p>	<p>Authentication is encrypted over a TLS 1.2 or higher connection to provide security between endpoints on every request to Exchange. You can control the scope by which Lightning Sync has access to your email service. To do so, limit which email service users are impersonated with your service account.</p>
Exchange admins must create a service account on your Exchange server to impersonate all syncing users.	<p>Lightning Sync uses the service account to query for users' Salesforce_Sync folders and their primary calendars. The service account also queries create, update, and read server content that users already have access to.</p> <p>Learn More</p>	<p>This design lets contacts and events sync without requiring users to log in to their individual Microsoft accounts. Such a design avoids time-outs to users' login sessions, offering a more reliable connection between systems.</p> <p>You can control the scope by which Lightning Sync has access to your email</p>

Requirement	Why it's required	Benefit to you
		<p>service. To do so, limit which email service users are impersonated with your service account.</p> <p>Learn More</p>
Service Account credentials must be provided on the Outlook Integration and Sync page in Salesforce Setup.	Salesforce encrypts the service account password field using 128-bit master keys, using the Advanced Encryption Standard (AES) algorithm.	<p>Only Salesforce admins with the permissions to access the Outlook Integration and Sync page in Setup can see or change the service account address.</p> <p>As the password is typed, it's masked to prevent others from seeing it. The contents can't be copied and pasted elsewhere. You can't learn what the service account password is by revisiting the page later.</p>

SEE ALSO:

[See the Big Picture for Setting Up Lightning Sync for Microsoft® Exchange Lightning Sync System Requirements](#)

OAuth 2.0 Connection for Microsoft Users

Connecting with OAuth 2.0 is available for Lightning Sync users working from Microsoft® Office 365®. To learn more, see the Lightning Sync system requirements.

Requirement	Why it's required	Benefit to you
Lightning Sync automatically requests its scope of access to all aspects of your users' Exchange mailbox and its resources.	While OAuth 2.0 provides access to more objects in your email service, Microsoft sets the breadth of that scope. Neither Salesforce nor Microsoft admins can adjust it. However, Lightning Sync can only read, write, and update contacts and events from users' email services. Lightning Sync isn't designed to discover or access other objects.	<p>Minimal setup is required to connect your applications using this method.</p> <p>This method provides access to users' Microsoft contacts and events without individual user authentication. As a result, sync between the applications remains consistent, and data is reliably updated in both systems without dependency on the user.</p>
Your company's Microsoft admin must provide access to Microsoft Office 365 from an account with global administrator permissions and accept Lightning Sync access to Microsoft.	After electing to connect using OAuth 2.0, you're redirected to https://login.microsoftonline.com to log in to your Office 365 email service. This site is	<p>Working hand-in-hand with the predetermined scope requirement, this method provides access to users' Microsoft contacts and events without individual user authentication. This benefit provides a sync experience with fewer interruptions.</p> <p>Several measures provide security for your data during transfer and within Salesforce.</p>

Requirement	Why it's required	Benefit to you
	<p>the Azure Active Directory portal for customers on global infrastructure databases, also known as Global Services. From the portal, you provide your global administrator credentials and accept permission to let Lightning Sync access your Microsoft account. This design ensures that your global administrator credentials are never stored in Salesforce.</p> <p>Next, you're redirected to the Outlook Integration and Sync page in Salesforce Setup, where your Microsoft Azure tenant ID is stored. Behind the scenes, Salesforce obtains an access token to your Microsoft account. The access token is required to gain read, update, create, or delete access to Microsoft contacts or events.</p> <p>Learn More</p>	<ul style="list-style-type: none"> • By design, your Azure tenant secrets are never in transmission with the OAuth 2.0 connection method. Instead, Salesforce handles the management of both public and private keys. • Your Microsoft tenant ID is encrypted at rest. It's visible only from the Outlook Integration and Sync page, so only Salesforce admins (or other users with Setup access) can see it. Plus, without signed Salesforce verification, interception of your tenant ID can't provide access to your Microsoft account. • The access token is securely transferred from your Microsoft account to Salesforce over a TLS connection. The token is encrypted, and expires every hour. New tokens are always transferred over a TLS connection. <p>Completing this process in no way provides impersonation rights to your global administrator account.</p>

SEE ALSO:

[See the Big Picture for Setting Up Lightning Sync for Microsoft® Exchange](#)

Connection for Google G Suite Users

The Google G Suite connection method is a combination of an OAuth 2.0 and a service account connection. This design is based on a method recommended by Google for connecting server to server.

Requirement	Why it's required	Benefit to you
<p>Your Google admin must establish a service account for your G Suite account. To do so, Google admins generate a private key that includes access to your Google contacts and calendar API. A Salesforce admin then uploads the key to Salesforce.</p>	<p>After Salesforce admins upload the private key, the key provides Salesforce with an access token to your company's Google account. This access is required for read, update, create, or delete access to Google contacts or events.</p> <p>See Also:</p> <ul style="list-style-type: none"> • Prepare Your Google Account for Lightning Sync 	<p>After they're uploaded, Google private keys are encrypted at rest. The private key signs the outbound sync requests sent from Salesforce. Requests can only be verified with the matching public key, possessed by your G Suite account.</p> <p>The generated access token is securely transferred from your Google account to Salesforce over a TLS connection. The token is encrypted. Every hour, the access token</p>

Requirement	Why it's required	Benefit to you
	<ul style="list-style-type: none"><li data-bbox="604 260 1019 289">• Prepare Salesforce for Lightning Sync	expires and a new token is transferred, always over a TLS connection.

SEE ALSO:

[See the Big Picture for Setting Up Lightning Sync for Microsoft® Exchange Lightning Sync System Requirements](#)

LIGHTNING SYNC TRANSACTIONS

Review the transactions made by Lightning Sync in response to the work your users complete in Salesforce, and the order in which they occur.

Lightning Sync initiates communication between Salesforce and your mail service asynchronously, so that the sync process doesn't slow down the users' intended Salesforce transaction.

- Changes made from Salesforce are queued for transmission to the email service.
- Changes made from the email service are retrieved by a periodic polling mechanism.

When contacts or events are synced to the opposite system, Lightning Sync impersonates the user who created or updated the original item. This behavior preserves accurate data on the items' last update.

For specific transaction details, review these scenarios.

Sync Contacts from Salesforce to Email Service

1. User creates a contact.
2. Asynchronous job is enqueued to sync the transaction. Lightning Sync:
 - a. Determines which users who are configured for sync should sync the contact.
 - b. Checks whether contact meets sync filters.
 - c. Calls the email service to see whether the contact exists.
 - i. If it does exist, the contact is updated in the email service.
 - ii. If the contact doesn't exist, Lightning Sync calls the email service to create the contact.
 - d. Matching contacts are mapped between Salesforce and the email service for future syncing.

Sync Events from Salesforce to Email Service

1. User creates an event.
2. Lightning Sync checks whether the user is set up to sync events.
3. Asynchronous job is enqueued to sync the transaction.
 - a. Lightning Sync checks whether the event meets sync filters.
 - b. Lightning Sync calls the email service to see whether the event exists.
 - i. If it does exist, the event is updated in the email service.
 - ii. If the event doesn't exist, Lightning Sync calls the email service to create the event.
 - c. Matching events are mapped between Salesforce and the email service for future syncing.

Sync Event Deletion from Salesforce to Email Service

1. User deletes an event.
2. Lightning Sync checks whether the record has been mapped to an event in the email service.
3. Lightning Sync checks whether the user is set up to have deleted events automatically removed from the other system.
4. If mapped to an event, asynchronous job is enqueued. Lightning Sync calls the mail service to delete the event.

Sync Contact or Event Creation, Update, or Deletion from Email Service to Salesforce

Lightning Sync runs a job for all syncing users semi-continuously. The number of syncing users impacts job frequency.

1. Lightning Sync checks whether contacts or events were created or updated, or whether events were deleted from the email service.
 - a. Lightning Sync checks for matched items to update. If items are discovered to have no match, new records are created in Salesforce.
 - b. For deleted events, Lightning Sync checks whether users are set up to have deleted events automatically removed from the opposite system. If so, the event is deleted from Salesforce.

SEE ALSO:

[How Your Contacts Sync with Lightning Sync](#)

[How Your Events Sync with Lightning Sync](#)