Set Up and Maintain Your Salesforce Organization

Salesforce, Winter '18

@salesforcedocs

Last updated: November 2, 2017

CONTENTS

SET UP AND MAINTAIN YOUR SALESFORCE ORGANIZATION

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

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: All Editions

IN THIS SECTION:

Try Out Salesforce

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

Plan Your Salesforce Rollout

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

Set Up Your Company in Salesforce

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

User Management

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

Control Who Sees What

Salesforce provides a flexible, layered data sharing design that allows you to expose different data sets to different sets of users, so users can do their job without seeing data they don't need to see. Use permission sets and profiles to specify the objects and fields users can access. Use organization-wide sharing settings, user roles, sharing rules to specify the individual records that users can view and edit.

Revoking Permissions and Access

Who Has Access to Account Records?

Cache Force.com Data

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

Protect Your Salesforce Organization

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

Monitor Your Organization

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

Enable Your Users to Work on Mobile Devices

Salesforce provides several mobile apps to keep you and your users connected and productive, no matter where you are.

Enable Salesforce Desktop for Your Organization

Learn More About Setting Up Salesforce

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

Try Out Salesforce

EDITIONS

Available in: Salesforce Classic

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

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

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

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

IN THIS SECTION:

Start a New Trial

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

Delete Trial Data

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

Start a New Trial

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

User Permissions Needed

To start a new trial:

- Modify All Data

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

You can start a new trial if you have:

- Fewer than 1,000 rows of data
- No additional user licenses added by Salesforce
- No additional functionality enabled by Salesforce

1. From Setup, enter `Start a New Trial` in the `Quick Find` box, then select **Start a New Trial**. This link is available only during your trial period.
2. Select your language and template preferences.
3. Enter the requested text stating that you want to abandon your current trial org and all its data, including sample data and data that you've entered.
4. To confirm that all of your current data will be lost, select the checkbox.
5. Click **Submit**.
6. When the confirmation page appears, click **Submit**.

Delete Trial Data

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To delete trial data:
- Modify All Data

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

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

- The user has the "Modify All Data" user permission.
- The org is in a trial state.
- The org doesn't have portals enabled.
- The user isn't a Partner Administrator, acting on another user's behalf.

1. From Setup, enter `Delete All Data` in the `Quick Find` box, then select **Delete All Data**.
2. Enter the requested text stating that you understand that all data in your org will be deleted, including sample data and data that you entered. Your user and admin setup isn't affected.
3. Click **Submit**.

Note: If data storage limits prevent you from deleting all your trial data this way, use Mass Delete Records to delete your accounts. Then use Delete All Data to delete your remaining trial data. For instructions for using Mass Delete Records, see Delete Multiple Records and Reports on page 486.

Plan Your Salesforce Rollout

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

If you're wondering how to get started, you might consider working with a consulting partner to take full advantage of the product. Consulting partners are firms that employ Salesforce-certified consultants. Consultants work with you to learn what your company needs, design and build your Salesforce organization to meet those needs, and test the organization before you roll it out to your teams. Consulting partners have one goal in mind: Your success with Salesforce.

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

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

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

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

Compare	Rolling out Salesforce Yourself	Rolling out Salesforce with a Partner
Qualifications	Sometimes companies have Salesforce-certified employees who can assist with setup.	Consultants are Salesforce-certified.

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

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

SEE ALSO:

Successfully Implement with Salesforce Partners

Successfully Implement with Salesforce Partners

Set Up Your Company in Salesforce

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

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

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To view company information:

- View Setup and Configuration

To change company information:

- Modify All Data

IN THIS SECTION:

Manage Information About Your Company

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

Allow the Required Domains

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

Customize the User Interface

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

Set Up the Lightning Experience Home Page

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

Select Your Language, Locale, and Currency

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

Define Your Fiscal Year

Specify a fiscal year that fits your business needs.

Set Up and Manage Search

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

Provide Maps and Location Services

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

Customize Reports and Dashboards

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

Respond to Critical Updates

Salesforce periodically releases updates that improve the performance, logic, and usability of Salesforce, but may affect your existing customizations. When these updates become available, Salesforce lists them in Setup at **Critical Updates** and displays a message when administrators go to Setup.

Organize Data with Divisions

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

Salesforce Upgrades and Maintenance

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

Permissions for UI Elements, Records, and Fields

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

How Do I Discontinue Service?

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

SEE ALSO:

Feature Licenses Overview

Permission Set Licenses

Usage-based Entitlements

Manage Information About Your Company

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

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

Field	Description
`Address`	Street address of the organization. Up to 255 characters are allowed in this field.
`Admin Newsletter`	Allow administrators in your organization to choose whether they want to receive administrator-targeted promotional emails from Salesforce.
`API Requests, Last 24 Hours`	The total number of API requests issued by the organization in the last 24 hours. The maximum number of requests depends on your Edition.
`City`	City in which organization is located. Up to 40 characters are allowed in this field.
`Corporate Currency`	The currency in which the organization's corporate headquarters reports revenue. Serves as the basis for all currency conversion rates. Only for organizations that use multiple currencies.
`Country`	Country portion of user's address. Entry is selected from a picklist of standard values, or entered as text. Up to 80 characters are allowed if the field is a text field.
`Created By`	User who signed up the organization, including creation date and time. (Read only)

Field	Description
Currency Locale	The country or geographic region in which the organization is located. The setting affects the format of currency amounts. For single currency organizations only.
Default Language	The default language that is selected for new users in the organization. This setting determines the language used for the user interface text and help. In all editions except Personal Edition and Database.com, individual users can separately set the language for their own login, which overrides the organization setting. In Group Edition, this field is called Display Language. This setting also determines the language in which all customizations—such as custom fields, tabs, and user interface options—are stored. For customizations, individual users' language settings don't override this setting. If you edit or clone existing filter criteria, check that this setting matches the default language that was configured when the filter criteria was originally set. Otherwise, the filter criteria can be evaluated differently than expected.
Default Locale	The default country or geographic region that is selected for new users in the organization. This setting determines the format of dates, times, and names in Salesforce. In Contact Manager, Group, Professional, Enterprise, Unlimited, Performance, and Developer Edition organizations, individual users can set their personal locale, which overrides the organization setting. In Group Edition, this field is called Locale.
Default Time Zone	Primary time zone in which the organization is located. A user's individual Time Zone setting overrides the organization's Default Time Zone setting. Note: Organizations in Arizona typically select "Mountain Standard Time," and organizations in parts of Indiana that don't follow Daylight Savings Time usually select "Eastern Standard Time."
Division	Group or division that uses the service, for example, PC Sales Group. Up to 40 characters are allowed in this field.
Fax	Fax number. Up to 40 characters are allowed in this field.
Fiscal Year Starts In	If using a standard fiscal year, the starting month and year for the organization's fiscal year. If using a custom fiscal year, the value is "Custom Fiscal Year."
Hide Notices About System Downtime	Select this checkbox to prevent advance notices about planned system downtime from displaying to users when they log in to Salesforce.

Field	Description
`Hide Notices About System Maintenance`	Select this checkbox to prevent advance notices about planned system maintenance from displaying to users when they log in to Salesforce.
`Modified By`	User who last changed the company information, including modification date and time. (Read only)
`Newsletter`	Allow users in your organization to choose whether they want to receive user-targeted promotional emails from Salesforce.
`Organization Edition`	Edition of the organization, such as Developer Edition or Enterprise Edition.
`Organization Name`	Name of the organization. Up to 80 characters are allowed in this field.
`Phone`	Main phone number at organization. Up to 40 characters are allowed in this field.
`Primary Contact`	Person who is main contact or administrator at the organization. You can enter a name, or select a name from a list of previously defined users. Up to 80 characters are allowed in this field.
`Restricted Logins, Current Month`	Number of restricted login users who have logged in during the current month. This value resets to zero at the beginning of each month. The maximum number of restricted login users for the organization is in parentheses.
`Salesforce Licenses`	Number of Salesforce user accounts that can be defined for access to the service. This number represents the Salesforce user licenses for which the organization is billed, if charges apply.
`Salesforce Organization ID`	Code that uniquely identifies your organization to Salesforce.
`State/Province`	State or province portion of user's address. Entry is selected from a picklist of standard values, or entered as text. Up to 80 characters are allowed if the field is a text field.
`Streaming API Events, Last 24 Hours`	The total number of Streaming API events used by the organization in the last 24 hours. The maximum number of events depends on your edition.
`Zip`	Zip or postal code of the organization. Up to 20 characters are allowed in this field.
`Used Data Space`	Amount of data storage in use. The value is expressed as a measurement (for example, 500 MB) and as a percentage of the total amount of data storage available (for example, 10%).

Field	Description
`Used File Space`	Amount of file storage in use. The value is expressed as a measurement (for example, 500 MB) and as a percentage of the total amount of file storage available (for example, 10%).

SEE ALSO:

Set Up Your Company in Salesforce

Allow the Required Domains

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: All Editions.

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

If you've disabled third-party cookies (typically enabled by default in all major browsers), you must accept them for Salesforce to function properly.

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

Salesforce uses these domains to deliver content.

- *.content.force.com
- *.force.com
- *.salesforce.com
- *.salesforceliveagent.com (used with Live Agent, Omni-Channel, and SOS)
- *.bluetail.salesforce.com
- In addition, these domains are used to deliver content in the right frame of your login screen.

- *.sfdcstatic.com
- secure.eloqua.com
- www.google.*
- *.doubleclick.net
- www.facebook.com
- ssl.google-analytics.com

The right frame content is displayed in the followings URLs.

- login.salesforce.com
- test.salesforce.com
- <yourInstance>.salesforce.com
- A My Domain URL without custom branding (for example, norns.my.salesforce.com)

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

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

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

34.224.144.232	52.21.43.255
34.197.49.208	52.54.5.76
52.44.146.48	54.236.191.28
34.225.107.166	52.21.109.221
34.206.188.121	107.23.62.176
54.210.4.174	107.23.102.197
54.208.220.233	54.87.200.56
52.73.79.3	52.86.60.223
52.22.254.22	34.200.157.195
34.193.204.122	52.205.154.40
52.4.158.80	52.54.242.233
52.3.73.106	54.175.157.145
34.205.234.140	34.195.58.231
107.23.108.83	34.196.109.221
54.82.148.169	52.22.224.140
52.4.238.209	52.72.252.194
107.21.49.246	52.203.119.68
34.200.8.4	107.23.29.15

EDITIONS

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

Customize the User Interface

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

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

IN THIS SECTION:

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To modify user interface settings:

- Customize Application

User Interface Settings

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

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To modify user interface settings:

- Customize Application

User Interface Settings

Enable Collapsible Sections

Collapsible sections let users collapse or expand sections on their record detail pages by using the arrow icon next to the section heading. When enabling collapsible sections, make sure your section headings are displayed for each page layout. Sections remain expanded or collapsed until the user changes the settings for that tab. If your org has enabled record types, Salesforce remembers a different setting for each record type.

Show Quick Create

The Quick Create area on a tab home page allows users to create a record quickly with minimal information. It displays by default on the tab home pages for leads, accounts, contacts, forecasts, and opportunities. You can control whether the Quick Create area is displayed on all relevant tab home pages.

Note: The `Show Quick Create` setting also affects whether users can create records from within the lookup dialog. Creating records in the lookup dialog is available only if Quick Create is available for your chosen record type. In addition, users always need the appropriate "Create" permission to use Quick Create even though it displays for all users.

Enable Hover Details

Hover detail displays an interactive overlay containing record details. Details appear when users hover over a link to that record in the Recent Items list on the sidebar, or in a lookup field on a record detail page. Users can quickly view information about a record before clicking to view or edit the record. The record's mini page layout determines which fields are included in the hover details. Users can't customize which fields appear. This option is enabled by default.

Note: To view hover details for a record, users need the appropriate sharing access, and field-level security access for the fields in the mini page layout.

Enable Related List Hover Links

Related list hover links display at the top of record detail pages and custom object detail pages in Setup. Users can hover over a related list link to display the list and its number of records in an interactive overlay. Users quickly view and manage the related list items from the overlay. Users can also click a related list hover link to jump to the related list without having to scroll down the patge. This option is enabled by default.

Enable Separate Loading of Related Lists

When enabled, users see primary record details immediately. As the related list data loads, users see a progress indicator. Separate loading can improve performance on record detail pages for orgs with large numbers of related lists. This option is disabled by default. The options for separately loading related lists don't apply to Visualforce pages, the Self-Service portal, or other pages for which you can't control the layout.

Enable Separate Loading of Related Lists of External Objects

When enabled, related lists of external objects are loaded separately from primary record details and related lists of standard and custom objects. External objects behave similarly to custom objects, except that they map to data that's stored outside your Salesforce org. It can take awhile to retrieve data from an external system, depending on the network latency and availability of the external system. The `Enable Separate Loading of Related Lists of External Objects` option is conveniently selected by default. The options for separately loading related lists don't apply to Visualforce pages, the Self-Service portal, or other pages for which you can't control the layout.

Enable Inline Editing

Inline editing lets users quickly edit field values, right on a record's detail page. This option is enabled by default and applies to all users in your org.

Note: This option doesn't enable inline editing for profiles. Select `Enable Enhanced Profile List Views` under Setup.

Enable Enhanced Lists

Enhanced lists give you the ability to quickly view, customize, and edit list data to speed up your daily productivity. When enabled with the `Enable Inline Editing` setting, users can also edit records directly from the list, without navigating away from the page. This option is enabled by default.

Note: To enable enhanced lists for profiles in particular, select `Enable Enhanced Profile List Views` under Setup.

Enable the Salesforce Classic 2010 User Interface Theme

This option is not related to Lightning Experience. In this case, "Salesforce Classic 2010 user interface theme" refers to the newer version of Salesforce Classic, which is the interface that immediately precedes Lightning Experience. Enabling this option turns on the updated Salesforce Classic look and feel. Disabling it turns on the Salesforce Classic 2005 user interface theme —the *classic, classic* Salesforce interface.

Warning: Some features, like Chatter, require the Salesforce Classic 2010 user interface theme. Disabling this theme automatically disables Chatter in both Salesforce Classic and Lightning Experience.

Only users with supported browsers see the Salesforce Classic 2010 user interface theme.

The Salesforce Classic 2010 user interface theme is not supported in portals or on the Console tab.

Enable Tab Bar Organizer

The Tab Bar Organizer arranges tabs in the main tab bar to prevent horizontal scrolling of the page. The Organizer dynamically determines how many tabs can display based on the width of the browser window. It puts tabs that extend beyond the browser's viewable area into a drop-down list.

Note: Note the following limitations:

- The Tab Bar Organizer isn't available with the partner portal or Customer Portal.

- The Tab Bar Organizer is only available with the Salesforce Classic 2010 user interface theme. Orgs using the Salesforce Classic 2005 user interface theme can enable the feature, but it isn't available to users until the newer theme is also enabled.
- The Tab Bar Organizer isn't available on Internet Explorer 6.

Enable Printable List Views

Printable list views let users easily print list views. If it's enabled, users click the **Printable View** link from any list view to open a new browser window, displaying the list view in a print-ready format. The link is located next to the **Help for this Page** link in the colored title bar of the page.

Enable Spell Checker on Tasks and Events

Available in all Editions. Enables the **Check Spelling** button when users create or edit tasks or events. The spell checker analyzes the `Description` field on events and the `Comments` field on tasks.

Enable Customization of Chatter User Profile Pages

Enables administrators to customize the tabs on the Chatter user profile page. This includes adding custom tabs or removing default tabs. If disabled, users see the Feed and Overview tabs only.

Sidebar Settings

Enable Collapsible Sidebar

The collapsible sidebar enables users to show or hide the sidebar on every page that normally includes it. When enabled, the collapsible sidebar is available to all users in your org, but each user can choose how to display the sidebar. Users can leave the sidebar visible, or they can collapse it and show it only when needed by clicking the edge of the collapsed sidebar.

Note: Call center users won't see incoming calls if they collapse the sidebar.

Tip: If your org uses divisions, we recommend that you keep the sidebar pinned and visible so you always have access to the Divisions drop-down list.

Show Custom Sidebar Components on All Pages

If you have custom home page layouts that include components in the sidebar, this option makes the sidebar components available on all pages for all org users. If you only want certain users to view sidebar components on all pages, grant those users the "Show Custom Sidebar On All Pages" permission.

Note: If the `Show Custom Sidebar Components on All Pages` user interface setting is selected, the "Show Custom Sidebar On All Pages" permission is not available.

Calendar Settings

Enable Home Page Hover Links for Events

Enables hover links in the calendar section of the Home tab. On the Home tab, users can hover the mouse over the subject of an event to see the details of the event in an interactive overlay. This option is enabled by default. This checkbox only controls the Home tab; hover links are always available on other calendar views.

The fields available in the event detail and edit overlays are defined in a mini page layout.

Note: If you create all day events, we recommend adding the `All Day Event` field to the events mini page layout.

Enable Drag-and-Drop Editing on Calendar Views

Enables dragging of events on single-user, daily and weekly calendar views. This allows users to reschedule events without leaving the page. This option is enabled by default.

Note: Calendar views can load less quickly when this checkbox is enabled.

Enable Click-and-Create Events on Calendar Views

Lets users create events on day and weekly calendar views by double-clicking a specific time slot and entering event details in an interactive overlay. The fields available in the event detail and edit overlays are defined in a mini page layout.

Recurring events and multi-person events aren't supported for click-and-create events on calendar views.

Enable Drag-and-Drop Scheduling on List Views

Lets users create events associated with records by dragging records from list views to weekly calendar views and entering event details in an interactive overlay. This option is disabled by default. The fields available in the event detail and edit overlays are defined in a mini page layout.

Enable Hover Links for My Tasks List

Enables hover links for tasks in the My Tasks section of the Home tab and on the calendar day view. This option is enabled by default. Users can hover the mouse over the subject of a task to see the details of that task in an interactive overlay.

Your administrator can configure the information presented on these overlays.

Setup Settings

Enable Enhanced Page Layout Editor

When enabled, the enhanced page layout editor replaces the current interface for editing page layouts with a feature-rich WYSIWYG editor that includes several improvements.

Enable Enhanced Profile List Views

Enables enhanced list views and inline editing on the profiles list page. With inline editing in enhanced profile list views, you can manage multiple profiles at once.

Enable Enhanced Profile User Interface

Enables the enhanced profile user interface, which allows you to easily navigate, search, and modify settings for a single profile.

Enable Streaming API

Enables Streaming API, which lets you receive notifications for changes to data that match a SOQL query that you define in a secure and scalable way. This field is selected by default. If your Salesforce edition has API access and you don't see this checkbox, contact Salesforce.

Enable Dynamic Streaming Channel Creation

Enables dynamic channel creation when using the generic streaming feature of Streaming API. When enabled, generic streaming channels get dynamically created when clients subscribe, if the channel hasn't already been created. This field is selected by default. If your Salesforce edition has API access and you don't see the checkbox, contact Salesforce.

Enable Custom Object Truncate

Enables truncating custom objects, which permanently removes all the records from a custom object while keeping the object and its metadata intact for future use.

Enable Improved Setup User Interface

When disabled, users with Salesforce Classic access their personal settings from the Setup menu. When enabled, users with Salesforce Classic access their personal settings from the My Settings menu, accessible from the username menu. The Setup link is also moved from the username menu to the Force.com App Menu. If you change this setting, be sure to notify all users in your org.

Enable Advanced Setup Search (Beta)

When enabled, users can search for Setup pages, custom profiles, permission sets, public groups, roles, and users from the sidebar in Setup. When disabled, users can search for Setup pages only.

Note:

- Advanced Setup Search is in beta; it is production quality but has known limitations.

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

Advanced Settings

Activate Extended Mail Merge

Enables Extended Mail Merge for your org. When selected, the **Mass Mail Merge** link is available in the Tools area on the home pages for accounts, contacts, and leads. Also, single mail merges requested from the Activity History related list on a record are performed using Extended Mail Merge functionality.

Extended Mail Merge is available by request only. Contact Salesforce Customer Support if you are interested in this feature.

Always save Extended Mail Merge documents to the Documents tab

Mail merge documents generated using Extended Mail Merge are added to the user's documents folder on the Documents tab, rather than delivered as email attachments. Users are sent confirmation emails when their mail merge requests have completed. Those emails include links for retrieving generated documents from the Documents tab. These documents count against your org's storage limits.

Set Up the User Interface in Salesforce Classic

EDITIONS

Available in: Salesforce Classe

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

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

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

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

  To access My Settings, click your name in the upper-right corner of any Salesforce page, then click **My Settings**. You can also access My Settings from your Chatter profile page: in the right pane, click **My Settings**.
- The My Settings home page includes quick links for easily accessing the most commonly used personal settings tools and tasks.

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

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

Note: The improved Setup user interface:

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

IN THIS SECTION:

Find Items in Setup with Advanced Setup Search (Beta)

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

SEE ALSO:

Personalize Your Salesforce Experience

Explore the Salesforce Setup Menu

Find Items in Setup with Advanced Setup Search (Beta)

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

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

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

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

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

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

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To enable Advanced Setup Search:

- Customize Application

To search Setup:

- View Setup and Configuration

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

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

IN THIS SECTION:

Setup Search Results Page (Beta)

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

Setup Search Results Page (Beta)

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

EDITIONS

Available in: Salesforce Classic

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

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

In the Setup Search Results page:

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

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

Tip: When viewing setup search results, bookmark the results page in your Web browser to easily perform the same search in the future. For example, if you often search for "smit", you can bookmark the results page to perform the same search again. The URL for this bookmark would be something like `https://`*`MyCompany`*`.salesforce.com/ui/setup/SetupSearchResultsPage?setupSearch=smit`.

SEE ALSO:

Find Items in Setup with Advanced Setup Search (Beta)

Set Up the Lightning Experience Home Page

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

EDITIONS

Available in: Lightning Experience

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

Create and edit Home pages from the Lightning App Builder. From Setup, enter *`Lightning App Builder`* in the `Quick Find` box, then select **Lightning App Builder**. Click **New** to create a Lightning Home page, or edit an existing page.

You can also access the Lightning App Builder directly from the Home page. Click ⚙ and select **Edit Page** to create a copy of the current Home page to edit.

IN THIS SECTION:

Set a New Default Home Page

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

Assign Custom Home Pages to Specific Profiles

Assign pages to different profiles to give your users access to a Home page perfect for their role.

Lightning Experience Home Permissions and Settings

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

Set a New Default Home Page

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

You can set the default Home page in two places.

- Lightning App Builder—From Setup, enter *`Lightning App Builder`* in the `Quick Find` box, then select **Lightning App Builder**.

  After you save a page, click **Activate** from the Page Saved dialog, or click **Activation** later.

- Home in Setup—From Setup, enter *`Home`* in the `Quick Find` box, then select **Home**.

  Click **Set Default Page** and select a page. To restore the standard Home page, select System Default.

EDITIONS

Available in: Lightning Experience

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

USER PERMISSIONS

To create and save Lightning Pages in the Lightning App Builder

- Customize Application

To view Lightning Pages in the Lightning App Builder

- View Setup and Configuration

Assign Custom Home Pages to Specific Profiles

Assign pages to different profiles to give your users access to a Home page perfect for their role.

You can set page assignments by profile in two places. You can use the Lightning App Builder to assign profiles to a single Home page, but Setup offers more control over page assignments.

- Lightning App Builder—From Setup, enter *`Lightning App Builder`* in the `Quick Find` box, then select **Lightning App Builder**.

  After you save a page, click **Activate** from the Page Saved dialog, or click **Activation** and select `Assign this Home page to specific profiles`.

- Home in Setup—From Setup, enter *`Home`* in the `Quick Find` box, then select **Home**.

  Click **Set Page Assignments** or click ▼ next to a profile and select **Change Assignment**.

EDITIONS

Available in: Lightning Experience

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

USER PERMISSIONS

To create and save Lightning Pages in the Lightning App Builder

- Customize Application

To view Lightning Pages in the Lightning App Builder

- View Setup and Configuration

Lightning Experience Home Permissions and Settings

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

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

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

The performance chart and Top Deals display opportunity information about a rep's sales team if they have an associated team. Otherwise, the chart displays opportunities owned by the rep.

Note: The performance chart isn't compatible with custom fiscal years. If you have custom fiscal years enabled in your org, create your own reports and dashboards to display on the Home page.

EDITIONS

Available in: Lightning Experience

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

To populate the performance chart, Top Deals, and the Assistant, users must have:

Table 1: Required Permissions for Home Features

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

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

SEE ALSO:

Set Up Accounts

Track Your Sales Performance

View Important Updates with the Assistant

Select Your Language, Locale, and Currency

EDITIONS

Available in: Salesforce Classic

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

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

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

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

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

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

IN THIS SECTION:

Language Settings Overview

Supported Locales

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

Supported Time Zones

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

Set Your Personal or Organization-Wide Currency

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

Edit Conversion Rates

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

Supported Currencies

Language Settings Overview

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

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

The Salesforce Web user interface has two language settings:

- Personal language—All on-screen text, images, buttons, and online help display in this language. Edit your personal information to change this setting.
- Default organization language—This applies to all new users until they select their personal language. This setting also determines the language in which all customizations—such as custom fields, tabs, and user interface options—are stored. For customizations, users' personal language settings don't override this default setting. Some setup items that are manually entered by an administrator can be translated in the Translation Workbench.

  Administrators can change this setting by editing the company information.

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

IN THIS SECTION:

Supported Languages

Salesforce offers three levels of language support: fully supported languages, end-user languages, and platform-only languages.

SEE ALSO:

Select Your Language, Locale, and Currency

Supported Languages

Salesforce offers three levels of language support: fully supported languages, end-user languages, and platform-only languages.

A two-character language code identifies each language, such as `en`, or a five-character locale code, such as en_AU.

Note: Setting a default locale is different from setting a default language.

In addition to the Salesforce language support, you can localize your org in two ways. Use the Translation Workbench to specify languages you want to translate, assign translators to languages, translate your text customizations, and override labels and translations from managed packages. You can translate everything from custom picklist values to custom fields so that your global users can use Salesforce in their language.

The second option is to rename tabs and fields in Salesforce. If your custom application uses only a few standard Salesforce tabs and fields, you can translate them.

Fully Supported Languages

You can change the language for all features, including Help, to one of the following fully supported languages from the Setup page. Enter *`Company Information`* in the Quick Find box, select **Company Information**, then select **Edit**.

- Chinese (Simplified): `zh_CN`
- Chinese (Traditional): `zh_TW`
- Danish: `da`
- Dutch: `nl_NL`
- English: `en_US`
- Finnish: `fi`
- French: `fr`
- German: `de`
- Italian: `it`
- Japanese: `ja`
- Korean: `ko`
- Norwegian: `no`
- Portuguese (Brazil): `pt_BR`
- Russian: `ru`
- Spanish: `es`
- Spanish (Mexico): `es_MX`
- Swedish: `sv`
- Thai: `th`

Note:

- Spanish (Mexico) falls back to Spanish for customer-defined translations.
- Even though the Salesforce user interface is fully translated to Thai, Help remains in English.

End-User Languages

End-user languages are useful if you have a multilingual organization or partners who speak languages other than your company's default language. For end-user languages, Salesforce provides translated labels for all standard objects and pages, *except* administrative pages, Setup, and Help. When you specify an end-user language, labels and Help that aren't translated appear in English. End-user languages are intended only for personal use by end users. Don't use end-user languages as corporate languages. Salesforce doesn't provide customer support in end-user languages.

End-user languages include:

- Arabic: `ar`
- Bulgarian: `bg`
- Croatian: `hr`
- Czech: `cs`
- English (UK): `en_GB`
- Greek: `el`
- Hebrew: `iw`
- Hungarian: `hu`

- Indonesian: `in`
- Polish: `pl`
- Portuguese (European): `pt_PT`
- Romanian: `ro`
- Slovak: `sk`
- Slovenian: `sl`
- Turkish: `tr`
- Ukrainian: `uk`
- Vietnamese: `vi`

Note: Salesforce provides limited support for right-to-left languages—Arabic and Hebrew—for the following features.

- Live Agent
- Cases
- Accounts

These features are not supported in Lightning Experience, the Salesforce app, any other mobile app or mobile browser, or any user interface except Salesforce Classic. There is no guarantee that right-to-left languages function correctly with any other Salesforce features. There are no plans to expand the list of supported features.

Features that aren't supported for right-to-left languages include, but are not limited to, the following.

- Report Builder
- Generating quote PDFs
- Customizable forecasting
- Emails
- Salesforce Knowledge
- Feeds
- Communities
- Certain search features, including lemmatization and synonym groups

The absence of a feature from this list does not imply support. Only Live Agent, Cases, and Accounts are supported with right-to-left languages.

Platform-Only Languages

In situations where Salesforce doesn't provide default translations, use platform-only languages to localize apps and custom functionality that you've built on the Salesforce App Cloud. You can translate items such as custom labels, custom objects, and field names. You can also rename most standard objects, labels, and fields. Informative text and non-field label text aren't translatable.

Platform-only languages are available in all places where you can select a language in the application. However, when you select a platform-only language, all standard Salesforce labels default to English or, in select cases, to an end-user or fully supported language.

When you specify a platform-only language, labels for standard objects and fields fall back to English, except:

- Dutch (Belgium) falls back to Dutch
- English (Australia), English (India), English (Malaysia), and English (Philippines) fall back to English (UK).
- French (Belgium), French (Canada), French (Luxembourg), and French (Switzerland) fall back to French.
- German (Austria), German (Belgium), German (Luxembourg), and German (Switzerland) fall back to German.
- Italian (Switzerland) falls back to Italian.

- Romanian (Moldova) falls back to Romanian.
- Montenegrin falls back to Serbian (Latin).
- Portuguese (European) falls back to Portuguese (Brazil).

The following platform-only languages are currently supported.

- Albanian: `sq`
- Arabic (Algeria): `ar_DZ`
- Arabic (Bahrain): `ar_BH`
- Arabic (Egypt): `ar_EG`
- Arabic (Iraq): `ar_IQ`
- Arabic (Jordan): `ar_JO`
- Arabic (Kuwait): `ar_KW`
- Arabic (Lebanon): `ar_LB`
- Arabic (Libya): `ar_LY`
- Arabic (Morocco): `ar_MA`
- Arabic (Oman): `ar_OM`
- Arabic (Qatar): `ar_QA`
- Arabic (Saudi Arabia): `ar_SA`
- Arabic (Sudan): `ar_SD`
- Arabic (Syria): `ar_SY`
- Arabic (Tunisia): `ar_TN`
- Arabic (United Arab Emirates): `ar_AE`
- Arabic (Yemen): `ar_YE`
- Armenian: `hy`
- Basque: `eu`
- Bosnian: `bs`
- Bengali: `bn`
- Catalan: `ca`
- Chinese (Simplified—Singapore): `zh_SG`
- Chinese (Traditional—Hong Kong): `zh_HK`
- Dutch (Belgium): `nl_BE`
- English (Australia): `en_AU`
- English (Canada): `en_CA`
- English (Hong Kong): `en_HK`
- English (India): `en_IN`
- English (Ireland): `en_IE`
- English (Malaysia): `en_MY`
- English (Philippines): `en_PH`
- English (Singapore): `en_SG`
- English (South Africa): `en_ZA`
- Estonian: `et`

- French (Belgium): `fr_BE`
- French (Canada): `fr_CA`
- French (Luxembourg): `fr_LU`
- French (Switzerland): `fr_CH`
- Georgian: `ka`
- German (Austria): `de_AT`
- German (Belgium): `de_BE`
- German (Luxembourg): `de_LU`
- German (Switzerland): `de_CH`
- Hindi: `hi`
- Icelandic: `is`
- Irish: `ga`
- Italian (Switzerland): `it_CH`
- Latvian: `lv`
- Lithuanian: `lt`
- Luxembourgish: `lb`
- Macedonian: `mk`
- Malay: `ms`
- Maltese: `mt`
- Romanian (Moldova): `ro_MD`
- Montenegrin: `sh_ME`
- Romansh: `rm`
- Serbian (Cyrillic): `sr`
- Serbian (Latin): `sh`
- Spanish (Argentina): `es_AR`
- Spanish (Bolivia): `es_BO`
- Spanish (Chile): `es_CL`
- Spanish (Colombia): `es_CO`
- Spanish (Costa Rica): `es_CR`
- Spanish (Dominican Republic): `es_DO`
- Spanish (Ecuador): `es_EC`
- Spanish (El Salvador): `es_SV`
- Spanish (Guatemala): `es_GT`
- Spanish (Honduras): `es_HN`
- Spanish (Nicaragua): `es_NI`
- Spanish (Panama): `es_PA`
- Spanish (Paraguay): `es_PY`
- Spanish (Peru): `es_PE`
- Spanish (Puerto Rico): `es_PR`
- Spanish (United States): `es_US`

- Spanish (Uruguay): `es_UY`
- Spanish (Venezuela): `es_VE`
- Tagalog: `tl`
- Tamil: `ta`
- Urdu: `ur`
- Welsh: `cy`

SEE ALSO:

Select Your Language, Locale, and Currency

Enable and Disable the Translation Workbench

Supported Locales

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

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
Albanian (Albania)	sq_AL	Albanian Lek: ALL	2008-02-28 4.30.PM	6.00.PD	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Arabic (Algeria)	ar_DZ	Algerian Dinar: DZD	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Arabic (Bahrain)	ar_BH	Bahraini Dinar: BHD	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To view company information:

- View Setup and Configuration

To change company information:

- Customize Application

The available personal setup options vary according to which Salesforce Edition you have.

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							Country
Arabic (Egypt)	ar_EG	Egyptian Pound: EGP	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Arabic (Iraq)	ar_IQ	Iraqi Dinar: IQD	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Arabic (Jordan)	ar_JO	Jordanian Dinar: JOD	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Arabic (Kuwait)	ar_KW	Kuwaiti Dinar: KWD	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Arabic (Lebanon)	ar_LB	Lebanese Pound: LBP	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Arabic (Libya)	ar_LY	Libyan Dinar: LYD	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Arabic (Morocco)	ar_MA	Moroccan Dirham: MAD	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							City, State ZipCode Country
Arabic (Oman)	ar_OM	Omani Rial: OMR	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Arabic (Qatar)	ar_QA	Qatar Rial: QAR	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Arabic (Saudi Arabia)	ar_SA	Saudi Arabian Riyal: SAR	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Arabic (Sudan)	ar_SD	Sudanese Pound: SDG	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Arabic (Syria)	ar_SY	Syrian Pound: SYP	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Arabic (Tunisia)	ar_TN	Tunisian Dinar: TND	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
Arabic (United Arab Emirates)	ar_AE	UAE Dirham: AED	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Arabic (Yemen)	ar_YE	Yemen Riyal: YER	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Armenian (Armenia)	hy_AM	Armenian Dram: AMD	25.10.2016, 17:00	06:00	1234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Azerbaijani (Azerbaijan)	az_AZ	Azerbaijanian New Manat: AZN	2008-02-28 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Basque (Spain)	eu_ES	Euro: EUR	2008-02-28 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Belarusian (Belarus)	be_BY	Belarussian Ruble: BYR	28.2.2008 16.30	6.00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Bengali (Bangladesh)	bn_BD	Bangladesh Taka: BDT	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							Country
Bosnian (Bosnia and Herzegovina)	bs_BA	Convertible Marks: BAM	28.02.2008. 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Bulgarian (Bulgaria)	bg_BG	Bulgarian Lev: BGN	25.10.2016 17:00	6:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Burmese (Myanmar [Burma])	my_MM	Myanmar Kyat: MMK	/ / :	:	, .	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Catalan (Spain, Euro)	ca_ES_EURO	Euro: EUR	28/02/2008 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Catalan (Spain)	ca_ES	Euro: EUR	28/02/2008 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Chinese (China, Pinyin Ordering)	zh_CN_PINYIN	Chinese Yuan: CNY	2008-2-28 PM4:30	上午6：00	1,234.56	LName FName	Country ZipCode State City Address Line 1, Address Line 2

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
Chinese (China, Stroke Ordering)	zh_CN_STROKE	Chinese Yuan: CNY	2008-2-28 PM4:30	上午6：00	1,234.56	LName FName	Country ZipCode State City Address Line 1, Address Line 2
Chinese (China)	zh_CN	Chinese Yuan: CNY	2008-2-28 PM4:30	上午6：00	1,234.56	LName FName	Country ZipCode State City Address Line 1, Address Line 2
Chinese (Hong Kong SAR China, Stroke Ordering)	zh_HK_STROKE	Hong Kong Dollar: HKD	25/10/2016 PM5:00	6:00	1,234.56	LName FName	Country ZipCode State City Address Line 1, Address Line 2
Chinese (Hong Kong SAR China)	zh_HK	Hong Kong Dollar: HKD	2008 2 28 PM4:30	6:00	1,234.56	LName FName	Country ZipCode State City Address Line 1, Address Line 2
Chinese (Macau SAR China)	zh_MO	Macau Pataca: MOP	25/10/2016 PM5:00	6:00	1,234.56	LName FName	Country ZipCode State City Address Line 1, Address Line 2
Chinese (Singapore)	zh_SG	Singapore Dollar: SGD	28/02/2008 PM 04:30	06:00	1,234.56	LName FName	Country ZipCode State City Address Line 1, Address Line 2
Chinese (Taiwan, Stroke Ordering)	zh_TW_STROKE	Taiwan Dollar: TWD	2008-2-28 PM 4:30	上午6:00	1,234.56	LName FName	Country ZipCode State City Address Line 1,

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							Address Line 2
Chinese (Taiwan)	zh_TW	Taiwan Dollar: TWD	2008-2-28 PM 4:30	上午 6:00	1,234.56	LName FName	Country ZipCode State City Address Line 1, Address Line 2
Croatian (Croatia)	hr_HR	Croatian Kuna: HRK	28.02.2008. 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Czech (Czech Republic)	cs_CZ	Czech Koruna: CZK	28.2.2008 16:30	6:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Danish (Denmark)	da_DK	Danish Krone: DKK	28-02-2008 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Dutch (Aruba)	nl_AW	Aruba Florin: AWG	28-2-2008 16:30	6:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Dutch (Belgium)	nl_BE	Euro: EUR	28/02/2008 16:30	6:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Dutch (Netherlands)	nl_NL	Euro: EUR	28-2-2008 16:30	6:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							City, State ZipCode Country
Dutch (Suriname)	nl_SR	Surinam Dollar: SRD	28-2-2008 16:30	6:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Dzongkha (Bhutan)	dz_BT	Bhutan Ngultrum: BTN	- - PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Antigua and Barbuda)	en_AG	East Caribbean Dollar: XCD	25/10/2016, 5:00 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Australia)	en_AU	Australian Dollar: AUD	28/02/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Bahamas)	en_BS	Bahamian Dollar: BSD	25/10/2016, 5:00 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Barbados)	en_BB	Barbados Dollar: BBD	28/02/2008 16:30	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
English (Belize)	en_BZ	Belize Dollar: BZD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Bermuda)	en_BM	Bermuda Dollar: BMD	28/02/2008 16:30	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Botswana)	en_BW	Botswana Pula: BWP	28/02/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Cameroon)	en_CM	CFA Franc (BEAC): XAF	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Canada)	en_CA	Canadian Dollar: CAD	28/02/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Cayman Islands)	en_KY	Cayman Islands Dollar: KYD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Eritrea)	en_ER	Eritrea Nakfa: ERN	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							Country
English (Falkland Islands)	en_FK	Falkland Islands Pound: FKP	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Fiji)	en_FJ	Fiji Dollar: FJD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Gambia)	en_GM	Gambian Dalasi: GMD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Ghana)	en_GH	Ghanaian Cedi: GHS	28/02/2008 16:30	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Gibraltar)	en_GI	Gibraltar Pound: GIP	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Guyana)	en_GY	Guyana Dollar: GYD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Hong Kong SAR China)	en_HK	Hong Kong Dollar: HKD	28/2/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							City, State ZipCode Country
English (India)	en_IN	Indian Rupee: INR	28/2/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Indonesia)	en_ID	Indonesian Rupiah: IDR	28/02/2008 16:30	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Ireland, Euro)	en_IE_EURO	Euro: EUR	28/02/2008 16:30	06:00	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Ireland)	en_IE	Euro: EUR	28/02/2008 16:30	06:00	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Jamaica)	en_JM	Jamaican Dollar: JMD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Kenya)	en_KE	Kenyan Shilling: KES	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
English (Liberia)	en_LR	Liberian Dollar: LRD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Madagascar)	en_MG	Malagasy Ariary: MGA	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Malawi)	en_MW	Malawi Kwacha: MWK	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Malaysia)	en_MY	Malaysian Ringgit: MYR	28/02/2008 16:30	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Mauritius)	en_MU	Mauritius Rupee: MUR	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Namibia)	en_NA	Namibian Dollar: NAD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (New Zealand)	en_NZ	New Zealand Dollar: NZD	28/02/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							Country
English (Nigeria)	en_NG	Nigerian Naira: NGN	28/02/2008 16:30	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Pakistan)	en_PK	Pakistani Rupee: PKR	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Papua New Guinea)	en_PG	Papua New Guinea Kina: PGK	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Philippines)	en_PH	Philippine Peso: PHP	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Rwanda)	en_RW	Rwanda Franc: RWF	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Saint Helena)	en_SH	St Helena Pound: SHP	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Samoa)	en_WS	Samoa Tala: WST	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							City, State ZipCode Country
English (Seychelles)	en_SC	Seychelles Rupee: SCR	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Sierra Leone)	en_SL	Sierra Leone Leone: SLL	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Singapore)	en_SG	Singapore Dollar: SGD	28/02/2008 16:30	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Sint Maarten (Dutch part))	en_SX	Neth Antilles Guilder: ANG	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Solomon Islands)	en_SB	Solomon Islands Dollar: SBD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (South Africa)	en_ZA	South African Rand: ZAR	2008/02/28 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
English (Swaziland)	en_SZ	Swaziland Lilageni: SZL	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Tanzania)	en_TZ	Tanzanian Shilling: TZS	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Tonga)	en_TO	Tonga Pa'anga: TOP	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Trinidad and Tobago)	en_TT	Trinidad&Tobago Dollar: TTD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (Uganda)	en_UG	Ugandan Shilling: UGX	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (United Kingdom)	en_GB	British Pound: GBP	28/02/2008 16:30	06:00	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
English (United States)	en_US	U.S. Dollar: USD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							Country
English (Vanuatu)	en_VU	Vanuatu Vatu: VUV	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Estonian (Estonia)	et_EE	Euro: EUR	28.02.2008 16:30	6:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Finnish (Finland, Euro)	fi_FI_EURO	Euro: EUR	28.2.2008 16:30	6:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Finnish (Finland)	fi_FI	Euro: EUR	28.2.2008 16:30	6:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
French (Belgium)	fr_BE	Euro: EUR	28/02/2008 16:30	6:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
French (Canada)	fr_CA	Canadian Dollar: CAD	2008-02-28 16:30	06:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
French (Comoros)	fr_KM	Comoros Franc: KMF	28/02/2008 16:30	06:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							City, State ZipCode Country
French (France, Euro)	fr_FR_EURO	Euro: EUR	28/02/2008 16:30	06:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
French (France)	fr_FR	Euro: EUR	28/02/2008 16:30	06:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
French (Guinea)	fr_GN	Guinea Franc: GNF	28/02/2008 16:30	06:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
French (Haiti)	fr_HT	Haiti Gourde: HTG	28/02/2008 16:30	06:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
French (Luxembourg)	fr_LU	Euro: EUR	28/02/2008 16:30	06:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
French (Mauritania)	fr_MR	Mauritania Ougulya: MRO	28/02/2008 16:30	06:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
French (Monaco)	fr_MC	Euro: EUR	28/02/2008 16:30	06:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
French (Switzerland)	fr_CH	Swiss Franc: CHF	28.02.2008 16:30	06:00	1'234.56	Ms. FName LName	Address Line 1, Address Line 2 City Country - State ZipCode
French (Wallis and Futuna)	fr_WF	Pacific Franc: XPF	28/02/2008 16:30	06:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Georgian (Georgia)	ka_GE	Georgia Lari: GEL	25.10.2016, 17:00	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
German (Austria, Euro)	de_AT_EURO	Euro: EUR	28.02.2008 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
German (Austria)	de_AT	Euro: EUR	28.02.2008 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
German (Germany, Euro)	de_DE_EURO	Euro: EUR	28.02.2008 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
German (Germany)	de_DE	Euro: EUR	28.02.2008 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
German (Luxembourg, Euro)	de_LU_EURO	Euro: EUR	28.02.2008 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
German (Luxembourg)	de_LU	Euro: EUR	28.02.2008 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
German (Switzerland)	de_CH	Swiss Franc: CHF	28.02.2008 16:30	06:00	1'234.56	Ms. FName LName	Address Line 1, Address Line 2 ZipCode City State Country
Greek (Greece)	el_GR	Euro: EUR	28/2/2008 4:30 PM	6:00 πμ	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Hebrew (Israel)	iw_IL	Israeli Shekel: ILS	16:30 28/02/2008	06:00	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Hindi (India)	hi_IN	Indian Rupee: INR	/ / : PM	:	, .	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
Hungarian (Hungary)	hu_HU	Hungarian Forint: HUF	2008.02.28. 16:30	6:00	1 234,56	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
Icelandic (Iceland)	is_IS	Iceland Krona: ISK	28.2.2008 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Indonesian (Indonesia)	in_ID	Indonesian Rupiah: IDR	28/02/2008 16:30	6:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Irish (Ireland)	ga_IE	Euro: EUR	28/02/2008 16:30	06:00	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Italian (Italy)	it_IT	Euro: EUR	28/02/2008 16.30	6.00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Italian (Switzerland)	it_CH	Swiss Franc: CHF	28.02.2008 16:30	06:00	1'234.56	Ms. FName LName	Address Line 1, Address Line 2 City Country - State ZipCode
Japanese (Japan)	ja_JP	Japanese Yen: JPY	2008/02/28 16:30	6:00	1,234.56	LName FName	Country ZipCode State City Address Line 1,

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							Address Line 2
Kazakh (Kazakhstan)	kk_KZ	Kazakhstan Tenge: KZT	28.02.2008 16:30	06:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Khmer (Cambodia)	km_KH	Cambodia Riel: KHR	28/2/2008, 16:30	6:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Kyrgyz (Kyrgyzstan)	ky_KG	Kyrgyzstan Som: KGS	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Korean (North Korea)	ko_KP	North Korean Won: KPW	2008. 2. 28 PM 4:30	오전 6:00	1,234.56	LName FName	Country ZipCode State City Address Line 1, Address Line 2
Korean (South Korea)	ko_KR	Korean Won: KRW	2008. 2. 28 PM 4:30	오전 6:00	1,234.56	LName FName	Country ZipCode State City Address Line 1, Address Line 2
Lao (Laos)	lo_LA	Lao Kip: LAK	25/10/2016, 17:00	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Latvian (Latvia)	lv_LV	Euro: EUR	28.02.2008 16:30	06:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							City, State ZipCode Country
Lithuanian (Lithuania)	lt_LT	Euro: EUR	2008.2.28 16.30	06.00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Luba-Katanga (Congo - Kinshasa)	lu_CD	Franc Congolais: CDF	25/10/2016 17:00	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Luxembourgish (Luxembourg)	lb_LU	Euro: EUR	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Macedonian (Macedonia)	mk_MK	Macedonian Denar: MKD	28.2.2008 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Malay (Brunei)	ms_BN	Brunei Dollar: BND	28/02/2008 4:30 PM	6:00 AM	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Malay (Malaysia)	ms_MY	Malaysian Ringgit: MYR	28/02/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
Maltese (Malta)	mt_MT	Euro: EUR	28/02/2008 16:30	06:00	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Nepali (Nepal)	ne_NP	Nepalese Rupee: NPR	- - :	:	, .	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Norwegian (Norway)	no_NO	Norwegian Krone: NOK	28.02.2008 16:30	06:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Pashto (Afghanistan)	ps_AF	Afghanistan Afghani (New): AFN	: / /	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Persian (Iran)	fa_IR	Iranian Rial: IRR	: / /	:		Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Polish (Poland)	pl_PL	Polish Zloty: PLN	28.02.2008 16:30	06:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Portuguese (Angola)	pt_AO	Angola Kwanza: AOA	28-02-2008 16:30	6:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							Country
Portuguese (Brazil)	pt_BR	Brazilian Real: BRL	28/02/2008 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Portuguese (Cape Verde)	pt_CV	Cape Verde Escudo: CVE	28-02-2008 16:30	6:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Portuguese (Mozambique)	pt_MZ	Mozambique New Metical: MZN	28/02/2008 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Portuguese (Portugal)	pt_PT	Euro: EUR	28-02-2008 16:30	6:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Portuguese (São Tomé and Príncipe)	pt_ST	Sao Tome Dobra: STD	28-02-2008 16:30	6:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Romanian (Moldova)	ro_MD	Moldovan Leu: MDL	28.02.2008, 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Romanian (Romania)	ro_RO	Romanian Leu (New): RON	28.02.2008 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							City, State ZipCode Country
Romansh (Switzerland)	rm_CH	Swiss Franc: CHF	28.02.2008 16:30	06:00	1’234.56	Ms. FName LName	Address Line 1, Address Line 2 City Country - State ZipCode
Rundi (Burundi)	rn_BI	Burundi Franc: BIF	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Russian (Russia)	ru_RU	Russian Rouble: RUB	28.02.2008 16:30	6:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Serbian (Bosnia and Herzegovina)	sr_BA	Convertible Marks: BAM	2008-02-28 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Serbian (Serbia)	sr_RS	Serbian Dinar: RSD	28.2.2008. 16.30	06.00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Serbian (Serbia and Montenegro)	sr_CS	Serbian Dinar: CSD	28.2.2008. 16.30	06.00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
Serbo-Croatian (Bosnia and Herzegovina)	sh_BA	U.S. Dollar: USD	28.02.2008. 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Serbo-Croatian (Montenegro)	sh_ME	U.S. Dollar: USD	28.02.2008. 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Serbo-Croatian (Serbia and Montenegro)	sh_CS	U.S. Dollar: USD	28.02.2008. 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Slovak (Slovakia)	sk_SK	Euro: EUR	28.2.2008 16:30	6:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Slovenian (Slovenia)	sl_SI	Euro: EUR	28.2.2008 16:30	6:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Somali (Djibouti)	so_DJ	Dijibouti Franc: DJF	28/02/2008 4:30 PM	6:00 sn.	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Somali (Somalia)	so_SO	Somali Shilling: SOS	28/02/2008 4:30 PM	6:00 sn.	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							Country
Spanish (Argentina)	es_AR	Argentine Peso: ARS	28/02/2008 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (Bolivia)	es_BO	Bolivian Boliviano: BOB	28-02-2008 04:30 PM	06:00 AM	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (Chile)	es_CL	Chilean Peso: CLP	28-02-2008 04:30 PM	06:00 AM	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (Colombia)	es_CO	Colombian Peso: COP	28/02/2008 04:30 PM	06:00 AM	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (Costa Rica)	es_CR	Costa Rica Colon: CRC	28/02/2008 04:30 PM	06:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (Cuba)	es_CU	Cuban Peso: CUP	28/02/2008 16:30	6:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (Dominican Republic)	es_DO	Dominican Peso: DOP	28/02/2008 04:30 PM	06:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							City, State ZipCode Country
Spanish (Ecuador)	es_EC	U.S. Dollar: USD	28/02/2008 04:30 PM	06:00 AM	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (El Salvador)	es_SV	El Salvador Colon: SVC	02-28-2008 04:30 PM	06:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (Guatemala)	es_GT	Guatemala Quetzal: GTQ	28/02/2008 04:30 PM	06:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (Honduras)	es_HN	Honduras Lempira: HNL	02-28-2008 04:30 PM	06:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (Mexico)	es_MX	Mexican Peso: MXN	28/02/2008 04:30 PM	06:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (Nicaragua)	es_NI	Nicaragua Cordoba: NIO	02-28-2008 04:30 PM	06:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
Spanish (Panama)	es_PA	Panama Balboa: PAB	02/28/2008 04:30 PM	06:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (Paraguay)	es_PY	Paraguayan Guarani: PYG	28/02/2008 04:30 PM	06:00 AM	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (Peru)	es_PE	Peruvian Nuevo Sol: PEN	28/02/2008 04:30 PM	06:00 AM	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (Puerto Rico)	es_PR	U.S. Dollar: USD	02-28-2008 04:30 PM	06:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (Spain, Euro)	es_ES_EURO	Euro: EUR	28/02/2008 16:30	6:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (Spain)	es_ES	Euro: EUR	28/02/2008 16:30	6:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (United States)	es_US	U.S. Dollar: USD	2/28/2008 4:30 PM	6:00 a.m.	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							Country
Spanish (Uruguay)	es_UY	Uruguayan New Peso: UYU	28/02/2008 04:30 PM	06:00 AM	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Spanish (Venezuela)	es_VE	Venezuelan Bolivar Fuerte: VEF	28/02/2008 04:30 PM	06:00 AM	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Swedish (Sweden)	sv_SE	Swedish Krona: SEK	2008-02-28 16:30	06:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Tagalog (Philippines)	tl_PH	Philippine Peso: PHP	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Tajik (Tajikistan)	tg_TJ	Tajik Somoni: TJS	2/28/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Tamil (India)	ta_IN	Indian Rupee: INR	2-28-2008 4:30 PM	6:00 am	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Tamil (Sri Lanka)	ta_LK	Sri Lanka Rupee: LKR	2-28-2008 4:30 PM	6:00 am	1,234.56	Ms. FName LName	Address Line 1, Address Line 2

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							City, State ZipCode Country
Thai (Thailand)	th_TH	Thai Baht: THB	28/2/2551, 16:30 น.	6:00 น.	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Tigrinya (Ethiopia)	ti_ET	Ethiopian Birr: ETB	28/02/2008 4:30 PM	6:00	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Turkish (Turkey)	tr_TR	Turkish Lira (New): TRY	28.02.2008 16:30	06:00	1.234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Ukrainian (Ukraine)	uk_UA	Ukraine Hryvnia: UAH	28.02.2008 16:30	6:00	1 234,56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Urdu (Pakistan)	ur_PK	Pakistani Rupee: PKR	28/2/2008 4:30 PM	6:00 AM	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Uzbek (LATN,UZ)	uz_LATN_UZ	Uzbekistan Sum: UZS	2008-02-28 16:30	06:00	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
Vietnamese (Vietnam)	vi_VN	Vietnam Dong: VND	16:30 28/02/2008	06:00	1.234,56	LName FName	Address Line 1, Address Line 2 City, State ZipCode Country
Welsh (United Kingdom)	cy_GB	British Pound: GBP	28/02/2008 16:30	06:00	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country
Yoruba (Benin)	yo_BJ	CFA Franc (BCEAO): XOF	28/02/2008 4:30 PM	6:00 Àár	1,234.56	Ms. FName LName	Address Line 1, Address Line 2 City, State ZipCode Country

SEE ALSO:

Select Your Language, Locale, and Currency

Supported Time Zones

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To view company information:

- View Setup and Configuration

To change company information:

- Customize Application

The available personal setup options vary according to which Salesforce Edition you have.

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

1. From your personal settings, enter `Time Zone` in the `Quick Find` box, then select **Language and Time Zone**. No results? Enter `Personal Information` in the `Quick Find` box, then select **Personal Information**. Then click **Edit**.
2. Click the Time Zone drop-down list for a list of supported time zones.

For reference, the Salesforce supported times zones and codes (in chronological order) are as follows:

Time Zone Code	Time Zone Name
GMT+14:00	Line Is. Time (Pacific/Kiritimati)
GMT+13:00	Phoenix Is.Time (Pacific/Enderbury)
GMT+13:00	Tonga Time (Pacific/Tongatapu)
GMT+12:45	Chatham Standard Time (Pacific/Chatham)
GMT+12:00	New Zealand Standard Time (Pacific/Auckland)
GMT+12:00	Fiji Time (Pacific/Fiji)
GMT+12:00	Petropavlovsk-Kamchatski Time (Asia/Kamchatka)
GMT+11:30	Norfolk Time (Pacific/Norfolk)
GMT+11:00	Lord Howe Standard Time (Australia/Lord_Howe)
GMT+11:00	Solomon Is. Time (Pacific/Guadalcanal)
GMT+10:30	Australian Central Standard Time ((South Australia) Australia/Adelaide)
GMT+10:00	Australian Eastern StandardTime (New South Wales) (Australia/Sydney)
GMT+10:00	Australian Eastern Standard Time (Queensland) (Australia/Brisbane)
GMT+09:30	Australian Central Standard Time (Northern Territory) (Australia/Darwin)
GMT+09:00	Korea Standard Time (Asia/Seoul)
GMT+09:00	Japan Standard Time (Asia/Tokyo)
GMT+08:00	Hong Kong Time (Asia/Hong_Kong)
GMT+08:00	Malaysia Time (Asia/Kuala_Lumpur)
GMT+08:00	Philippines Time (Asia/Manila)
GMT+08:00	China Standard Time (Asia/Shanghai)

Time Zone Code	Time Zone Name
GMT+08:00	Singapore Time (Asia/Singapore)
GMT+08:00	China Standard Time (Asia/Taipei)
GMT+08:00	Australian Western Standard Time (Australia/Perth)
GMT+07:00	Indochina Time (Asia/Bangkok)
GMT+07:00	Indochina Time (Asia/Ho_Chi_Minh)
GMT+07:00	West Indonesia Time (Asia/Jakarta)
GMT+06:30	Myanmar Time (Asia/Rangoon)
GMT+06:00	Bangladesh Time (Asia/Dhaka)
GMT+05:45	Nepal Time (Asia/Kathmandu)
GMT+05:30	India Standard Time (Asia/Colombo)
GMT+05:30	India Standard Time (Asia/Kolkata)
GMT+05:00	Pakistan Time (Asia/Karachi)
GMT+05:00	Uzbekistan Time (Asia/Tashkent)
GMT+05:00	Yekaterinburg Time (Asia/Yekaterinburg)
GMT+04:30	Afghanistan Time (Asia/Kabul)
GMT+04:00	Azerbaijan Summer Time (Asia/Baku)
GMT+04:00	Gulf Standard Time (Asia/Dubai)
GMT+04:00	Georgia Time (Asia/Tbilisi)
GMT+04:00	Armenia Time (Asia/Yerevan)
GMT+03:30	Iran Daylight Time (Asia/Tehran)
GMT+03:00	East African Time (Africa/Nairobi)
GMT+03:00	Arabia Standard Time (Asia/Baghdad)
GMT+03:00	Arabia Standard Time (Asia/Kuwait)
GMT+03:00	Arabia Standard Time (Asia/Riyadh)
GMT+03:00	Moscow Standard Time (Europe/Minsk)
GMT+03:00	Moscow Standard Time (Europe/Moscow)
GMT+03:00	Eastern European Summer Time (Africa/Cairo)
GMT+03:00	Eastern European Summer Time (Asia/Beirut)
GMT+03:00	Israel Daylight Time (Asia/Jerusalem)
GMT+03:00	Eastern European Summer Time (Europe/Athens)

Time Zone Code	Time Zone Name
GMT+03:00	Eastern European Summer Time (Europe/Bucharest)
GMT+03:00	Eastern European Summer Time (Europe/Helsinki)
GMT+03:00	Eastern European Summer Time (Europe/Istanbul)
GMT+02:00	South Africa Standard Time (Africa/Johannesburg)
GMT+02:00	Central European Summer Time (Europe/Amsterdam)
GMT+02:00	Central European Summer Time (Europe/Berlin)
GMT+02:00	Central European Summer Time (Europe/Brussels)
GMT+02:00	Central European Summer Time (Europe/Paris)
GMT+02:00	Central European Summer Time (Europe/Prague)
GMT+02:00	Central European Summer Time (Europe/Rome)
GMT+01:00	Western European Summer Time (Europe/Lisbon)
GMT+01:00	Central European Time (Africa/Algiers)
GMT+01:00	British Summer Time (Europe/London)
GMT–01:00	Cape Verde Time (Atlantic/Cape_Verde)
GMT+00:00	Western European Time (Africa/Casablanca)
GMT+00:00	Irish Summer Time (Europe/Dublin)
GMT+00:00	Greenwich Mean Time (GMT)
GMT–00:00	Eastern Greenland Summer Time (America/Scoresbysund)
GMT–00:00	Azores Summer Time (Atlantic/Azores)
GMT–02:00	South Georgia Standard Time (Atlantic/South_Georgia)
GMT–02:30	Newfoundland Daylight Time (America/St_Johns)
GMT–03:00	Brasilia Summer Time (America/Sao_Paulo)
GMT–03:00	Argentina Time (America/Argentina/Buenos_Aires)
GMT–03:00	Chile Summer Time (America/Santiago)
GMT–03:00	Atlantic Daylight Time (America/Halifax)
GMT–04:00	Atlantic Standard Time (America/Puerto_Rico)
GMT–04:00	Atlantic Daylight Time (Atlantic/Bermuda)
GMT–04:30	Venezuela Time (America/Caracas)
GMT–04:00	Eastern Daylight Time (America/Indiana/Indianapolis)
GMT–04:00	Eastern Daylight Time (America/New_York)

Time Zone Code	Time Zone Name
GMT–05:00	Colombia Time (America/Bogota)
GMT–05:00	Peru Time (America/Lima)
GMT–05:00	Eastern Standard Time (America/Panama)
GMT–05:00	Central Daylight Time (America/Mexico_City)
GMT–05:00	Central Daylight Time (America/Chicago)
GMT–06:00	Central Standard Time (America/El_Salvador)
GMT–06:00	Mountain Daylight Time (America/Denver)
GMT–06:00	Mountain Standard Time (America/Mazatlan)
GMT–07:00	Mountain Standard Time (America/Phoenix)
GMT–07:00	Pacific Daylight Time (America/Los_Angeles)
GMT–07:00	Pacific Daylight Time (America/Tijuana)
GMT–08:00	Pitcairn Standard Time (Pacific/Pitcairn)
GMT–08:00	Alaska Daylight Time (America/Anchorage)
GMT–09:00	Gambier Time (Pacific/Gambier)
GMT–9:00	Hawaii-Aleutian Standard Time (America/Adak)
GMT–09:30	Marquesas Time (Pacific/Marquesas)
GMT–10:00	Hawaii-Aleutian Standard Time (Pacific/Honolulu)
GMT–11:00	Niue Time (Pacific/Niue)
GMT–11:00	Samoa Standard Time (Pacific/Pago_Pago)

SEE ALSO:

Select Your Language, Locale, and Currency

Set Your Personal or Organization-Wide Currency

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

EDITIONS

Available in: both Salesforce Classic and Lightning Experience.

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

USER PERMISSIONS

To view currencies:

- View Setup and Configuration

To change currencies:

- Customize Application

IN THIS SECTION:

Set Your Currency Locale

If you have a single-currency organization, you can set your default currency.

Set Your Corporate Currency

In multi-currency organizations, set your corporate currency to the currency in which your corporate headquarters reports revenue. All conversion rates are based on the corporate currency.

Set Your Personal Currency

In multi-currency organizations, you can set a personal currency that's different from the organization's corporate currency.

SEE ALSO:

Select Your Language, Locale, and Currency

Edit Conversion Rates

Supported Currencies

Supported Locales

Set Your Currency Locale

If you have a single-currency organization, you can set your default currency.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view currencies:

- View Setup and Configuration

To change currencies:

- Customize Application

1. Search Setup for Company Information.
2. On the Company Information page, click **Edit**.
3. Select a locale from the Currency Locale drop-down list.
4. Click **Save**.

Set Your Corporate Currency

In multi-currency organizations, set your corporate currency to the currency in which your corporate headquarters reports revenue. All conversion rates are based on the corporate currency.

When Support enables multiple currencies, your corporate currency is set to the value specified on the Company Information page in Setup. You can change the corporate currency.

1. Search Setup for Manage Currencies.
2. On the Currency page, click **Change Corporate**.
3. Select a currency from the New Corporate Currency drop-down list.
4. Click **Save**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view currencies:

- View Setup and Configuration

To change currencies:

- Customize Application

Set Your Personal Currency

In multi-currency organizations, you can set a personal currency that's different from the organization's corporate currency.

1. From your personal settings, enter `Time Zone` in the `Quick Find` box, then select **Language and Time Zone**. No results? Enter `Personal Information` in the `Quick Find` box, then select **Personal Information**.
2. Select a currency from the Currency drop-down list.
3. Save your changes.

SEE ALSO:

Personalize Your Salesforce Experience

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To view company information:

- View Setup and Configuration

To change company information:

- Customize Application

The available personal setup options vary according to which Salesforce Edition you have.

Edit Conversion Rates

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

1. Search Setup for Manage Currencies.
2. If you use advanced currency management, click **Manage Currencies**.
3. In the Active Currencies or Inactive Currencies list, click **Edit Rates**.
4. Enter the conversion rate between each currency and your corporate currency.
5. Click **Save**.

When you change the conversion rates, currency amounts are updated using the new rates. Previous conversion rates are not stored. All conversions within opportunities, forecasts, and other amounts use the current conversion rate.

If your organization uses advanced currency management, you can also manage dated exchange rates for currency fields on opportunities and opportunity products.

Note:

- You cannot track revenue gain or loss based on currency fluctuations.
- Changing conversion rates causes a mass recalculation of roll-up summary fields. This recalculation can take up to 30 minutes, depending on the number of records affected.
- You can also change a conversion rate via the API. However, if another roll-up summary recalculation for the same currency field is in progress, the age of that job affects the recalculation job that you triggered. Here's what happens when you request a currency rate change via the API, and a related job is in progress.
  - If the other recalculation for the same currency field was kicked off less than 24 hours ago, your currency rate change isn't saved. You can try again later or instead change the currency rate from Manage Currencies in Setup. Initiating the change from Setup stops the old job and triggers your recalculation to run.
  - If the other recalculation job was kicked off more than 24 hours ago, you can save your currency rate change and your job starts.

To check the status of your recalculation job, see the Background Jobs page in Setup.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To view currencies:

- View Setup and Configuration

To change currencies:

- Customize Application

SEE ALSO:

Set Your Personal or Organization-Wide Currency

About Advanced Currency Management

Supported Currencies

Salesforce supported currencies:

Currency Name	Currency Code
UAE Dirham	AED
Afghanistan Afghani (New)	AFN
Albanian Lek	ALL
Armenian Dram	AMD
Neth Antilles Guilder	ANG
Angola Kwanza	AOA
Argentine Peso	ARS
Australian Dollar	AUD
Aruba Florin	AWG
Azerbaijanian New Manat	AZN
Convertible Marks	BAM
Barbados Dollar	BBD
Bangladesh Taka	BDT
Bulgaria Lev	BGN
Bahraini Dinar	BHD
Burundi Franc	BIF
Bermuda Dollar	BMD
Brunei Dollar	BND
Bolivian Boliviano	BOB
Bolivia Mvdol	BOV
Brazilian Cruzeiro (old)	BRB
Brazilian Real	BRL
Bahamian Dollar	BSD
Bhutan Ngultrum	BTN
Botswana Pula	BWP
Belarussian Ruble	BYR
Belize Dollar	BZD
Canadian Dollar	CAD

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To view company information:

- View Setup and Configuration

To change company information:

- Customize Application

The available personal setup options vary according to which Salesforce Edition you have.

Currency Name	Currency Code
Franc Congolais	CDF
Swiss Franc	CHF
Unidades de fomento	CLF
Chilean Peso	CLP
Chinese Yuan	CNY
Colombian Peso	COP
Costa Rica Colon	CRC
Cuban Peso	CUP
Cape Verde Escudo	CVE
Czech Koruna	CZK
Dijibouti Franc	DJF
Danish Krone	DKK
Dominican Peso	DOP
Algerian Dinar	DZD
Estonian Kroon	EEK
Egyptian Pound	EGP
Eritrea Nakfa	ERN
Ethiopian Birr	ETB
Euro	EUR
Fiji Dollar	FJD
Falkland Islands Pound	FKP
British Pound	GBP
Georgia Lari	GEL
Ghanian Cedi	GHS
Gibraltar Pound	GIP
Gambian Dalasi	GMD
Guinea Franc	GNF
Guatemala Quetzal	GTQ
Guyana Dollar	GYD
Hong Kong Dollar	HKD

Currency Name	Currency Code
Honduras Lempira	HNL
Croatian Kuna	HRK
Haiti Gourde	HTG
Hungarian Forint	HUF
Indonesian Rupiah	IDR
Israeli Shekel	ILS
Indian Rupee	INR
Iraqi Dinar	IQD
Iranian Rial	IRR
Iceland Krona	ISK
Jamaican Dollar	JMD
Jordanian Dinar	JOD
Japanese Yen	JPY
Kenyan Shilling	KES
Kyrgyzstan Som	KGS
Cambodia Riel	KHR
Comoros Franc	KMF
North Korean Won	KPW
Korean Won	KRW
Kuwaiti Dinar	KWD
Cayman Islands Dollar	KYD
Kazakhstan Tenge	KZT
Lao Kip	LAK
Lebanese Pound	LBP
Sri Lanka Rupee	LKR
Liberian Dollar	LRD
Lesotho Loti	LSL
Libyan Dinar	LYD
Moroccan Dirham	MAD
Moldovan Leu	MDL

Currency Name	Currency Code
Malagasy Ariary	MGA
Macedonian Denar	MKD
Myanmar Kyat	MMK
Mongolian Tugrik	MNT
Macau Pataca	MOP
Mauritania Ougulya	MRO
Mauritius Rupee	MUR
Maldives Rufiyaa	MVR
Malawi Kwacha	MWK
Mexican Peso	MXN
Mexican Unidad de Inversion (UDI)	MXV
Malaysian Ringgit	MYR
Mozambique New Metical	MZN
Namibian Dollar	NAD
Nigerian Naira	NGN
Nicaragua Cordoba	NIO
Norwegian Krone	NOK
Nepalese Rupee	NPR
New Zealand Dollar	NZD
Omani Rial	OMR
Panama Balboa	PAB
Peruvian Nuevo Sol	PEN
Papua New Guinea Kina	PGK
Philippine Peso	PHP
Pakistani Rupee	PKR
Polish Zloty	PLN
Paraguayan Guarani	PYG
Qatar Rial	QAR
Romanian Leu (New)	RON
Serbian Dinar	RSD

Currency Name	Currency Code
Russian Rouble	RUB
Rwanda Franc	RWF
Saudi Arabian Riyal	SAR
Solomon Islands Dollar	SBD
Seychelles Rupee	SCR
Sudanese Pound	SDG
Swedish Krona	SEK
Singapore Dollar	SGD
St Helena Pound	SHP
Sierra Leone Leone	SLL
Somali Shilling	SOS
Surinam Dollar	SRD
South Sudan Pound	SSP
Sao Tome Dobra	STD
Syrian Pound	SYP
Swaziland Lilageni	SZL
Thai Baht	THB
Tajik Somoni	TJS
Turkmenistan New Manat	TMT
Tunisian Dinar	TND
Tonga Pa'anga	TOP
Turkish Lira (New)	TRY
Trinidad&Tobago Dollar	TTD
Taiwan Dollar	TWD
Tanzanian Shilling	TZS
Ukraine Hryvnia	UAH
Ugandan Shilling	UGX
U.S. Dollar	USD
Uruguayan New Peso	UYU
Uzbekistan Sum	UZS

Currency Name	Currency Code
Venezuelan Bolivar Fuerte	VEF
Vietnam Dong	VND
Vanuatu Vatu	VUV
Samoa Tala	WST
CFA Franc (BEAC)	XAF
East Caribbean Dollar	XCD
CFA Franc (BCEAO)	XOF
Pacific Franc	XPF
Yemen Riyal	YER
South African Rand	ZAR
Zambian Kwacha (New)	ZMK
Zimbabwe Dollar	ZWL

SEE ALSO:

Set Your Personal or Organization-Wide Currency

Define Your Fiscal Year

Specify a fiscal year that fits your business needs.

If your fiscal year follows the Gregorian calendar, but does not start in January, you can define a standard fiscal year with a different starting month. If your fiscal year follows a different structure from the Gregorian calendar, you can define a custom fiscal year that meets your needs.

Whether you use a standard fiscal year or a custom fiscal year, you define individual fiscal years one time. These fiscal year definitions allow you to use these fiscal periods throughout Salesforce including in reporting, opportunities, and forecasting.

Tip: As a best practice, update product schedules whenever a custom fiscal year is created or changed.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To define or edit fiscal years:
- Customize Application

To view fiscal years:
- View Setup and Configuration

Standard Fiscal Years

Standard fiscal years follow the Gregorian calendar, but can start on the first day of any month of the year.

Custom Fiscal Years

Some companies break down their fiscal years, quarters, and weeks into custom fiscal periods based on their financial planning requirements. Salesforce allows you to flexibly define these periods using custom fiscal years. For example, you can create a 13-week quarter represented by three periods of four, four, and five weeks, rather than calendar months.

If you use a common fiscal year structure, such as 4-4-5 or a 13-period structure, you can rapidly define a fiscal year. Just specify a start date and choose an included template. If the fiscal year structure you need is not among the templates, you can easily modify a template to suit your business. For example, if you use three fiscal quarters per year (a trimester) rather than four, delete or modify quarters and periods to meet your needs.

Your custom fiscal periods can be named based on your standards. For example, a fiscal period could be called "P2" or "February."

Fiscal years can be modified any time. For example, you can add an extra week to synchronize a custom fiscal year with a standard calendar in a leap year. Changes to fiscal year structure take effect immediately upon being saved. If you use forecasting, Salesforce recalculates your forecasts when you save changes to a fiscal year.

Considerations for Enabling Custom Fiscal Years

Before enabling custom fiscal years, consider these key points.

- After you enable custom fiscal years, you can't disable the feature. However, to revert to standard fiscal years, you can define custom fiscal years that follow the same Gregorian calendar structure as the Salesforce standard fiscal years.
- Fiscal year definitions are not automatically created. Define a custom fiscal year for each year you do business.
- Enabling or defining custom fiscal years impacts your forecasts, reports, and quotas.
  - When you define the first custom fiscal year, all existing forecasts, forecast history, and forecast adjustments from the year's first period forward are deleted. Forecasts for periods before the first custom fiscal year are not deleted and can be accessed as usual.
  - When you define a new custom fiscal year, any existing forecasts, forecast history, forecast adjustments, and quotas for the corresponding standard fiscal year are lost.
  - If you use Customizable Forecasting, you can group reports for a period after the last defined fiscal year only by date, not by period.
  - If you use Customizable Forecasting, view the forecast for the period included in the report before running a forecast report. Verify that your reports have the most updated amounts. If you use Collaborative Forecasts, it is not necessary to view the forecast before running reports.
- You can't use fiscal period columns in opportunity, opportunity with product, or opportunity with schedule reports.
- Opportunity list views don't include a fiscal period column.
- When custom fiscal years are enabled, you can't use the `FISCAL_MONTH()`, `FISCAL_QUARTER()`, or `FISCAL_YEAR()` date functions in SOQL.

IN THIS SECTION:

Set the Fiscal Year

If your company follows the Gregorian calendar year but you want to change the fiscal year start month, use standard fiscal years. If your company does not observe a standard fiscal year, you can enable custom fiscal years, which define a more complex fiscal year structure.

Customize the Fiscal Year Structure

If your custom fiscal year needs a different structure than one available from the templates, modify the details of your custom fiscal year definition.

Customize the Fiscal Year Labels

Customize the labels of your fiscal years in two ways: Naming schemes and prefix choices or fiscal year picklist customization.

Choosing a Custom Fiscal Year Template

Define a Custom Fiscal Year

Set up your company's custom fiscal years to fit your company's calendar. If you define a custom fiscal year and want to change it, edit the existing fiscal year definition.

Set the Fiscal Year

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view fiscal year:
- View Setup and Configuration

To change fiscal year:
- Customize Application

If your company follows the Gregorian calendar year but you want to change the fiscal year start month, use standard fiscal years. If your company does not observe a standard fiscal year, you can enable custom fiscal years, which define a more complex fiscal year structure.

Warning:

- Users of Customizable Forecasting: If you change your fiscal start month, you can lose all quotas, forecast history, and overrides. To preserve your data, change to a month previously used as the first month in a quarter. For example, if your start month is April and you change it to May, which isn't a month that starts a fiscal quarter, you lose data. If you change it to July, which is a month that starts a fiscal quarter, you preserve your data.
- Users of Collaborative Forecasts: If you change your fiscal year start month, quota and adjustment information is purged.

1. Back up your current data and export it into a set of comma-separated values (CSV) files.

   Tip: Run a data backup export because changing the fiscal year causes fiscal periods to shift. This change affects opportunities and forecasts organization-wide.

2. From Setup, enter *`Fiscal Year`* in the `Quick Find` box, then select **Fiscal Year**.
3. Select `Standard Fiscal Year` or `Custom Fiscal Year`.
   - To create a standard fiscal year, choose the start month. Then specify whether the fiscal year name is based on the year in which it begins or ends.

     If you want to apply the new fiscal year settings to your existing forecasts and quotas, select `Apply to All Forecasts and Quotas`. Whether this option is available depends on your forecast settings.

   - To create a custom fiscal year, click **Enable Custom Fiscal Years**, click **OK**, and define your fiscal year. See Define a Custom Fiscal Year.

     Warning: Custom fiscal years cannot be disabled once enabled. Enabling custom fiscal years has impacts on your reports, forecasts, quotas, and other date-sensitive material. Do not enable custom fiscal years unless you understand and are prepared for all the implications. For detailed information on the impact, see Define Your Fiscal Year.

4. Click **Save**.

For specific information on both types of fiscal years, see Define Your Fiscal Year on page 70.

Customize the Fiscal Year Structure

If your custom fiscal year needs a different structure than one available from the templates, modify the details of your custom fiscal year definition.

Custom fiscal years let you:

- Customize the period labels
- Reset the fiscal year to a template
- Add or remove fiscal periods
- Change the length of a fiscal week

Warning: Changing the length of a fiscal year has an impact on forecasting and reporting. For detailed information on the impact, see Define Your Fiscal Year.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To define or edit fiscal years:

- Customize Application

To view fiscal years:

- View Setup and Configuration

Customizing the Period Labels

You can change labels, or names of your fiscal year periods. Forecasting and reporting also use these period labels. For information about changing them, see Customize the Fiscal Year Labels on page 74.

Resetting the Fiscal Year to a Template

During customization, if you want to return to a fiscal year template, select a template from the `Reset Fiscal Year Structure` drop-down list.

Note: Resetting the fiscal year structure to a template removes all the customizations you made to the fiscal year.

Adding or Removing Fiscal Periods

You can easily add or remove fiscal periods (such as quarters, periods, or weeks) from the fiscal year structure.

To add fiscal periods:

1. From Setup, click **Company Profile** > **Fiscal Year**.
2. Click **Edit** for the fiscal year you want to edit.
3. If it is not already expanded, expand the **Advanced Customization** section.
4. Select the checkbox for the period before the new period. For example, to add a quarter, and you want it to be the second quarter, select the checkbox for the first quarter.
5. Click **Insert**.

   Note: The maximum number of fiscal periods is 250.

To remove a fiscal period:

1. From Setup, click **Company Profile** > **Fiscal Year**.
2. Click **Edit** for the fiscal year you want to edit.
3. If it is not already expanded, expand the **Advanced Customization** section.
4. Select the checkbox for the period you want to delete.
5. Click **Delete**.

Note: You must have at least one quarter, one period, and one week. If you delete a fiscal period or quarter, you delete forecast adjustments and quotas for that period or quarter.

Changing the Length of a Fiscal Week

To change the length of fiscal periods:

1. From Setup, click **Company Profile** > **Fiscal Year**.
2. Click **Edit** for the fiscal year you want to edit.
3. If it is not already expanded, expand the **Advanced Customization** section.
4. Choose the length from the **Duration** drop-down list for the fiscal week.

Note: To change the duration of a fiscal period or quarter, insert or delete weeks, or change the length of weeks that compose the period or quarter.

After you have customized your fiscal year, preview the fiscal year definition. Then, save your work.

Customize the Fiscal Year Labels

Customize the labels of your fiscal years in two ways: Naming schemes and prefix choices or fiscal year picklist customization.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions except Database.com

USER PERMISSIONS

To define or edit fiscal years:
- Customize Application

To view fiscal years:
- View Setup and Configuration

Fiscal Year Naming Schemes and Prefix Choices

When defining a custom fiscal year, you can choose the labeling scheme to use for your custom fiscal year. Each fiscal period type (quarter, period, and week) has a list of labeling schemes that you can select.

Quarter Name Scheme

Numbered by Year

This option allows you to add the quarter number to the quarter label. The quarter label is a combination of the label for the quarter prefix and the quarter number. For example, if the quarter prefix is "Q", the label for the third quarter Q3. To customize the quarter prefix, see `Quarter Prefix` on page 75. By default the order of the quarter determines its number (the first quarter is labeled "1"). To customize the order, select a different value from the quarter detail drop-down list.

Custom Quarter Names

This option allows you to set the quarter label to any name. The quarter label is set to the name you select from `Quarter Name`. By default the order of the quarter names is the same as the picklist order. To customize the order, select a different value from the quarter detail drop-down list.

Period Name Scheme

Numbered By Year

This option allows you to set the period label based on its position in the year. The period label is a combination of the period prefix and the period number. Period numbers do not reset in each quarter. For example, if the period prefix is "P," the label for the sixth period is P6. To customize the `Period Prefix`, see `Period Prefix` on page 75. By default the order of the period determines its number (the first period is labeled "1"). To customize the number, select a different value from the period detail drop-down list.

Numbered By Quarter

This option allows you to set the period label based on its position in the quarter. The period label is a combination of the period prefix and the period number. Period numbers reset in each quarter. For example, if the period prefix is "P," and the sixth period is the second period in the second quarter, its label is P2. To customize the period prefix, see `Period Prefix` on page 75. By default the number for each period is set by their order within the quarter (the first period in a quarter is labeled "1"); customize it by selecting a different value from the period detail drop-down list.

Standard Month Names

This option allows you to set the period label to the month name of the start of the period. For example, if a period started on October 12 and ends on November 10, the period label would be October.

Custom Period Names

This option allows you to set the period label to any string. The period label is set to the string you select from `Period Name`. By default the order of the period names is the same as the picklist order, which you can customize by selecting a different value from the period detail drop-down list.

Fiscal Year Picklists

Review these custom picklists to customize the labels for your custom fiscal year.

`Quarter Prefix`

The quarter prefix picklist is a list of options for the text that prefixes the quarter number or name if your fiscal year uses the **Numbered By Year** quarter naming scheme. For example, if the fiscal quarter is called "Q4," the "Q" is the quarter prefix.

`Period Prefix`

The period prefix picklist is a list of options for the text that prefixes the period number or name if your fiscal year uses the **Numbered By Year** period naming scheme. For example, if the fiscal quarter is called "P4," the "P" is the period prefix.

`Quarter Name`

The quarter name picklist is a list of options for the quarter name if your fiscal year uses the **Custom Quarter Names** quarter naming scheme. For example, if you want to name your quarters for the seasons (Spring, Summer, Fall, and Winter), you could set the quarter name list to those values.

`Period Name`

The period name picklist is a list of options for the quarter name if your fiscal year uses the **Custom Period Names** quarter naming scheme. Similar to the quarter name picklist, you can choose meaningful names for the period name picklist.

Customizing Fiscal Year Names

To customize one of these picklists:

1. From Setup, click **Company Profile** > **Fiscal Year**.
2. Click **Edit** next to the appropriate picklist.

SEE ALSO:

Define Your Fiscal Year

Choosing a Custom Fiscal Year Template

When defining a new custom fiscal year, your first step is to choose a custom fiscal year template. These templates are available to make it easier for you to define your custom fiscal year. They create a simple custom fiscal year that you can customize to meet your exact needs.

Note: If you choose a template and realize that it is not the best one for your fiscal year definition, you can reset it at any time using the **Reset Fiscal Year Structure** option.

Choose one of three types of templates:

4 Quarters per Year, 13 Weeks per Quarter

Choose one of these templates for your fiscal year if you want each quarter to have the same number of weeks per quarter. These templates all have 4 quarters, 12 periods, and 52 weeks per year. Each quarter is 13 weeks long and is composed of three periods. Two of the periods in each quarter are 4 weeks, and one is 5 weeks. In a 4-4-5 template, for example, the first and second period of a quarter are 4 weeks long, and the third period is 5 weeks long. Weeks are always 7 days long. A typical customization for these templates is to add extra weeks for leap years.

4-4-5

Within each quarter, period 1 has 4 weeks, period 2 has 4 weeks, and period 3 has 5 weeks

4-5-4

Within each quarter, period 1 has 4 weeks, period 2 has 5 weeks, and period 3 has 4 weeks

5-4-4

Within each quarter, period 1 has 5 weeks, period 2 has 4 weeks, and period 3 has 4 weeks

13 Periods per Year, 4 Weeks per Period

Choose one of these templates if your fiscal year has more than 12 periods and if one quarter is longer than the other quarters. These templates all have 4 quarters per year, 13 periods per year, 3 or 4 periods per quarter, 53 weeks per year, and 4 weeks per period (5 weeks in the final period). Weeks generally have 7 days, but include a short week at the end of a year. The most common customization for this type of template is to create or change the length of a short week.

3-3-3-4

Quarter 1 has 3 periods, quarter 2 has 3 periods, quarter 3 has 3 periods, and quarter 4 has 4 periods

3-3-4-3

Quarter 1 has 3 periods, quarter 2 has 3 periods, quarter 3 has 4 periods, and quarter 4 has 3 periods

3-4-3-3

Quarter 1 has 3 periods, quarter 2 has 4 periods, quarter 3 has 3 periods, and quarter 4 has 3 periods

4-3-3-3

Quarter 1 has 4 periods, quarter 2 has 3 periods, quarter 3 has 3 periods, and quarter 4 has 3 periods

Gregorian Calendar

12 months/year, standard Gregorian calendar.

Unlike the other template styles, you can't do advanced customization of a fiscal year that has been created from a Gregorian calendar template. Only use this template if you want to create a fiscal year that follows the Gregorian calendar. This template mimics the functionality of standard fiscal years.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To change your fiscal year:

- Customize Application

SEE ALSO:

Define Your Fiscal Year

Define a Custom Fiscal Year

Set up your company's custom fiscal years to fit your company's calendar. If you define a custom fiscal year and want to change it, edit the existing fiscal year definition.

Before defining a custom fiscal year, enable custom fiscal years. See Set the Fiscal Year on page 72 for more information.

Before defining or editing any custom fiscal years, be aware of its impact on forecasting, reports, and other objects by reviewing Define Your Fiscal Year on page 70.

Custom fiscal years cannot be deleted.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To view fiscal year:
- View Setup and Configuration

To change your fiscal year:
- Customize Application

Define a New Custom Fiscal Year

1. From Setup, click **Company Profile** > **Fiscal Year**.
2. Click **New**. The Custom Fiscal Year template dialog opens.
3. Choose a template and click **Continue** to close the Custom Fiscal Year template dialog. For more information on the templates, see Choosing a Custom Fiscal Year Template on page 76.
4. Set the fiscal year start date, the fiscal year name, and choose the week start day. You can also add a description for the fiscal year.

   Note: For the first custom fiscal year, the `Fiscal Year Start Date` and the `Week Start Date` are automatically set to today's date and day of week. If you already defined a custom fiscal year, the start dates are set to the day after the last end date of your custom fiscal years.

   To change other than the start date, year name, or week start day, see Customize the Fiscal Year Structure on page 73.

5. To review the fiscal year definition, click **Preview**.

   If it is correct, close the preview and click **Save** to save your fiscal year, or **Save & New** to save your fiscal year and define another fiscal year.

Warning: If your company uses forecasting, creating the first custom fiscal year deletes any quotas and adjustments in the corresponding and subsequent standard fiscal years.

Edit a Custom Fiscal Year

1. From Setup, click **Company Profile** > **Fiscal Year**.
2. Click a defined fiscal year name to review the details. Close the fiscal year preview to continue.
3. Click **Edit** for the fiscal year you want to edit.
4. Change the `Fiscal Year Start Date`, the `Fiscal Year Name`, `Description`, or `Week Start Day`.

   Sometimes changing the `Fiscal Year Start Date` causes this fiscal year to overlap with the previous fiscal year or create a gap between the fiscal years. In this case, the end date of the previous fiscal year is changed to the day before the start of this fiscal year.

   If changing the end date causes this fiscal year to overlap the next fiscal year, or create a gap between the fiscal years, the start date of the next fiscal year changes to the day after the end of this fiscal year.

   Note: You can't change the start or end date of a fiscal year if that causes it to overlap with a fiscal year that is defined using a Gregorian year template.

Warning: If you change the start or end date of any quarter, period, or week, you lose all forecast data that are within that date range, including quotas, forecast history, and forecast adjustments. It also includes all forecasts for date ranges automatically adjusted as a result of that change and end or start date changes resulting from inserting or deleting periods.

5. Click **Preview**.
6. Review the fiscal year definition. If it is correct, close the preview and click **Save** to save your fiscal year. To make more detailed edits, see Customize the Fiscal Year Structure on page 73.

   Note: The default label values for the fiscal year periods determine the fiscal year period labels for forecasting and reporting, unless you specify them. To change them, see Customize the Fiscal Year Labels on page 74.

Set Up and Manage Search

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

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

IN THIS SECTION:

Searchable Objects and Fields

Salesforce searches a unique set of fields for each object.

Configure Lookup Search

Choose which columns appear to users in the lookup search results.

Configure Synonym Groups

A search for one term in a synonym group returns results for all terms in the group. For example, a search for *USB drive* returns results for all terms in the synonym group, which contains *USB drive*, *thumb drive*, *flash stick*, and *memory stick*. Synonym groups remove the guesswork for users searching for records.

Configure Search Settings in Salesforce Classic

Enable document content search, CJKT search optimization, sidebar search auto-complete, and more. Configure the lookup settings and the number of search results per object and lookup settings.

Configure Search Results Filters in Salesforce Classic

Admins choose the filters available to users for refining search results. Choosing the correct filters for each object is important so that users can easily navigate through search results to find the right record.

Set Up and Manage Federated Search

Do your users search for content stored outside of Salesforce? Federated search makes it easy to add external search engines (or connectors) to your org. Users look for information using Salesforce global search and see external results in a single search results page. Understand more about how federated search works, how to set it up, and how users see results.

Help Users Find Missing Records

Are users reporting that records aren’t appearing in their search results? Admins can troubleshoot common search issues for users. Encouraging users to narrow their search scope or use more specific search terms is always a good first step. Admins can also verify the search status, permissions, and search settings. Learn about search result crowding, also called truncation, and how it affects the results returned.

Make Search Faster

Disabling search for custom objects and external objects and scheduling bulk uploads during off-peak hours helps speed up search.

Searchable Objects and Fields

Salesforce searches a unique set of fields for each object.

Note: When you search for a value in a field that's hidden from you by field-level security, your results include the record that contains the field. However, you can't see the field.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

The types of records you can search vary according to the edition you have.

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

IN THIS SECTION:

Searchable Fields by Object in Lightning Experience

The records included in search results depend on whether the record’s object type and its fields are searchable. If you search for an object with a value that’s stored in a field that isn’t searchable, your desired object doesn’t appear in your search results.

Searchable Fields by Object in Salesforce Classic

Each search type—sidebar, advanced, global, and lookup—searches a unique set of fields for each object. Your search results for a particular object depend on two factors: the type of search and the searchable fields for that object.

Searchable Fields by Object in Lightning Experience

The records included in search results depend on whether the record’s object type and its fields are searchable. If you search for an object with a value that’s stored in a field that isn’t searchable, your desired object doesn’t appear in your search results.

EDITIONS

Available in: Lightning Experience

The types of records you can search vary according to the edition you have.

Note: When you search for a value in a field that's hidden from you by field-level security, your results include the record that contains the field. However, you can't see the field.

Not all object and fields are searchable, so reference the table to determine which records you can find with Salesforce search.

Object	Fields
Account	**Account Name** **Account Name (Local)** **Account Number** **Account Site** **Billing Address** **Description** **Fax** **Phone** **Shipping Address** **Ticker Symbol** **Website** All custom fields

Object	Fields
Analytics (Dashboard and Lens)	Note: Analytic dashboard and lens search results appear under **Analytics**. Dashboard **Title** Lens **Description** **Developer Name** **Master Label** **Name**
Article (Knowledge Article)	**Article Number** **Summary** **Title** **URL Name** Attached file's content (text within the file) Attached file **Title**
Asset	**Asset Name** **Description** **Serial Number**
Campaign	**Campaign Name** **Description**
Case	**Case Number** **Description** **Subject** **Web Company** (of person who submitted the case online) **Web Email** (of person who submitted the case online) **Web Name** (of person who submitted the case online) **Web Phone** (of person who submitted the case online)
Channel Program	**Description** **Name**
Channel Program Level	**Channel Program Level**
Chatter (Feed)	@*Name* (where *Name* is a username)

Object	Fields
	Comment Body **Commenter Name** **File Name** **Group Name** **Links** **Post Body** **Post Origin (Person, Group, Record Name)**
Group (Chatter Group)	**Description** **Name**
Contact	**Assistant** **Asst. Phone** **Department** **Description** **Email** **Fax** **First Name (Local)** **Home Phone** **Last Name (Local)** **Mailing Address** **Mobile** **Other Address** **Other Phone** **Phone** **Title**
Contract	**Billing Address** **Billing Name** **Contract Name** **Contract Number** **Description** **Shipping Address** **Special Terms**
Custom objects and fields	**Name**

Object	Fields
	All custom auto-number fields and custom fields that are set as an external ID (no need to enter leading zeros) All custom fields of type email and phone All custom fields of type text, text area, long text area, and rich text area Note: Custom object records are searchable in the Salesforce user interface only if the custom object is associated with a custom tab. Users aren't required to add the tab for display. The same field types are also searchable for custom fields on standard objects. If an object has custom fields, you can find records of that object with the custom field values.
Dashboard	**Title**
Entitlement	**Entitlement Name**
External objects	Global search only: Text, text area, and long text area fields Note: • Lookup search isn’t available for external lookup relationship fields. To edit an external lookup relationship field, manually enter the value of the `External ID` standard field for the parent record. This limitation doesn’t apply when the parent external object is associated with the cross-org adapter for Salesforce Connect. • Lookup search isn’t available for indirect lookup relationship fields. To edit an indirect lookup relationship field, manually enter the value of the target field of the parent record. The target field is the custom field with `External ID` and `Unique` attributes that was selected when the indirect lookup relationship was created. To determine related records, Salesforce matches target field values against the values of the indirect lookup relationship field on the child object. An external object accesses data that’s stored outside your Salesforce org. Your Salesforce admin controls which external objects are searchable. Which external object fields are searched depends on how the external system handles searches. If the search results aren’t as you expected, use case-sensitive search strings that contain only alphanumeric characters. If the results still aren’t as expected, contact your admin for recommendations on searching your specific external system.
Event (Calendar)	**Description** **Subject**
File	**Body** **Description** **Extension** (such as ppt) **Name** **Owner**
Lead	**Address** **Company** **Company(Local)**

Object	Fields
	Description **Email** **Fax** **First Name (Local)** **Last Name (Local)** **Mobile** **Name** **Phone** **Title** Note: In Lightning Experience, both the converted lead record and the new record based on the converted lead are searchable. However, you can’t view or edit the converted lead record from the search results page.
Note	**Body** **Title**
Operating Hours	**Description** **Name**
Opportunity	**Description** **Opportunity Name**
Order	**Billing Address** **Description** **Order Name** **Order Number** **Order Reference Number** **PO Number** **Shipping Address**
Partner Fund Allocation	**Name** **Description**
Partner Fund Claim	**Partner Fund Claim**
Partner Fund Request	**Name** **Description** **Desired Outcome**

Object	Fields
Partner Marketing Budget	**Name** **Description**
People	**About Me** **Address** **Email** **Name** **Nickname** **Phone** **Title** **Username**
Person Account	**Account Name** **Account Name (Local)** **Account Number** **Account Site** **Assistant** **Assistant Phone** **Billing Address** **Description** **Email** **Fax** **Home Phone** **Mailing Address** **Mobile** **Other Address** **Other Phone** **Shipping Address** **Ticker Symbol** **Title** **Website** Note: The Person Account object contains fields that originate from both the Business Account and Contact objects. All search terms are compared to business account and contact fields at the same time.
Price Book	**Description**

Object	Fields
	Price Book Name
Product	**Product Code** **Product Description** **Product Name**
Quote	**Quote Name** **Quote Number**
Report	**Description** **Report Name**
Service Appointment	**Appointment Number** **Description** **Subject**
Service Crew	**Name**
Service Crew Member	**Name**
Service Resource	**Description** **Name**
Service Territory	**Description** **Name**
Task	**Comments** **Subject**
Topic	**Description** **Topic Name**
Work Order	**Description** **Subject** **Work Order Number**

IN THIS SECTION:

Searchable Setup Objects in Lightning Experience

EDITIONS

Available in: Lightning Experience

The types of records you can search vary according to the edition you have.

Use global search while in Setup to find specific setup records, such as the Lead Source picklist or the Sales Rep profile. Global search differs from Quick Find, which finds pages within the Setup menu, such as Account Settings or Profiles.

Within Setup, enter a name, and select the **in Setup** option in instant results or press Enter. When you search in Setup, using certain key words includes results from related searches. For example, when you search `Record Types` or `Search Layouts`, you also see results for `Object Manager`.

Top Results includes results from the Setup object pages you use most frequently. See results for a specific object by clicking the object's name on the left side of the page, under Search Results.

The following Setup objects are always shown in search results. You can't customize the order.

- Users
- Profiles
- Permission Sets
- Objects
- Fields
- Groups and Queues

If you want to see results for a Setup object not shown, use the **Show More** dropdown below the list. Here's a list of all the searchable Setup objects.

- Approval Post Templates
- Approval Processes
- Assignment Rules
- Business Hours
- Compact Layouts
- Custom Buttons or Links
- Custom Home Pages
- Duplicate Rules
- Email Alerts
- Email Templates
- Entitlement Process
- Field Updates
- Fields
- Groups and Queues
- Home Page Components
- Permission Sets
- Profiles

- Objects
- Roles
- Static Resources
- Users
- Workflow Outbound Messages
- Workflow Rules
- Workflow Tasks

Here are the columns shown in search results. You can't customize the columns. The Type column lists the type of setup record, such as Field. The Object field shows the Salesforce object, such as Contact.

- Name
- Type
- Object
- Last Modified Date
- Last Modified By

Setup search results have certain restrictions.

- You can't sort or filter results.
- You can only search by the API name of the setup record.

Searchable Fields by Object in Salesforce Classic

Each search type—sidebar, advanced, global, and lookup—searches a unique set of fields for each object. Your search results for a particular object depend on two factors: the type of search and the searchable fields for that object.

A few things to note about searchable fields:

- You can't search encrypted, formula, and lookup fields.
- By default, enhanced lookups query a limited set of fields, primarily *Name* fields for each object. If available in the enhanced lookup search dialog, select **All Fields** and enter other search terms unique to the record, to search through all searchable fields.

EDITIONS

Available in: Salesforce Classic

The types of records you can search vary according to the edition you have.

This table shows the types of search supported for each object. Not all fields are searchable, so follow the links to see the list of searchable fields for each object.

Object	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search	Global Search
Activities (Events and Tasks)	✓	✓			✓
Asset	✓	✓	✓		✓
Attachment	✓	✓			✓
Business Account	✓	✓	✓	✓	✓
Campaign	✓	✓	✓		✓
Case	✓	✓	✓		✓

Object	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search	Global Search
Channel Program	✓	✓	✓		✓
Channel Program Level	✓	✓			✓
Chatter Feed					✓
Chatter Group					✓
Coaching	✓	✓			✓
Community			✓		
Contact	✓	✓	✓	✓	✓
Salesforce CRM Content					✓
Contract	✓	✓	✓		✓
Contract Line Item	✓	✓			✓
Custom Object	✓	✓	✓	✓	✓
D&B Company	✓	✓			✓
Discussion			✓		
Document			✓		✓
Entitlement	✓	✓	✓		✓
External Object					✓
File					✓
Goal	✓	✓			✓
Idea	✓	✓	✓		✓
Knowledge Article					✓
Lead	✓	✓	✓		✓
Live Chat Transcript		✓			✓
Macro	✓	✓			✓
Metric	✓	✓			✓
Note	✓	✓			✓
Operating Hours	✓	✓	✓	✓	✓
Opportunity	✓	✓	✓	✓	✓
Order	✓	✓			✓

Object	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search	Global Search
Partner Fund Allocation	✓	✓	✓		✓
Partner Fund Claim	✓	✓			✓
Partner Fund Request	✓	✓	✓		✓
Partner Marketing Budget	✓	✓	✓		✓
People	✓	✓	✓		✓
Performance Cycle	✓	✓			✓
Person Account	✓	✓	✓	✓	✓
Price Book			✓		
Product			✓		✓
Question	✓	✓			✓
Quick Text	✓	✓			✓
Quote	✓	✓	✓		✓
Report	✓	✓			✓
Resource Absence	✓	✓		✓	✓
Reward Fund	✓	✓			✓
Reward Fund Type	✓	✓			✓
Self-Service User			✓		
Service Appointment	✓	✓		✓	✓
Service Contract	✓	✓			✓
Service Crew	✓	✓	✓		✓
Service Crew Member	✓	✓	✓		✓
Service Resource	✓	✓	✓	✓	✓
Service Resource Skill	✓	✓		✓	✓
Service Territory	✓	✓	✓	✓	✓
Service Territory Member	✓	✓		✓	✓
Skill	✓	✓			✓

Object	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search	Global Search
Solution			✓		✓
Thanks Badge	✓	✓			✓
Topic	✓	✓			✓
User	✓	✓	✓	✓	✓
Work.com Feedback	✓	✓			✓
Work Order	✓	✓	✓	✓	✓
Work Order Line Item	✓	✓	✓	✓	✓

Searchable Fields: Activities (Events and Tasks)

EDITIONS

Available in: Salesforce Classic

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

Note: Archived events and tasks aren't searchable.

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Comments` (tasks only)		✓	✓
`Description` (events only)		✓	✓
`Subject`	✓	✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓	✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓	✓

Searchable Fields: Asset

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Global Search
`Asset Name`	✓	✓	✓	✓
`Description`		✓		✓
`Serial Number`	✓	✓	✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓		✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓		✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Attachment

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Description`		✓	✓
`File Name`	✓	✓	✓

The contents of attachments are not searchable.

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Business Account

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
Account Name	✓	✓	✓	✓	✓
Account Name (Local)	✓	✓	✓	✓	✓
Account Number	✓	✓			✓
Account Site	✓	✓		✓	✓
Billing Address		✓			✓
Description		✓			✓
D-U-N-S Number (This field is only available to organizations that use Data.com Prospector)		✓			✓
Fax	✓	✓			✓
Phone	✓	✓			✓
Shipping Address		✓			✓
Ticker Symbol	✓	✓			✓
Website	✓	✓		✓	✓
All custom auto-number fields and custom fields	✓	✓			✓

EDITIONS

Available in: Salesforce Classic

The available business account fields vary according to which Salesforce edition you have.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
that are set as an external ID (You don't need to enter leading zeros.)					
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓			✓

Searchable Fields: Campaign

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Global Search
`Campaign Name`	✓	✓	✓	✓
`Description`		✓		✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓		✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓		✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Case

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Global Search
`Case Comments`		✓		✓
`Case Number` (You don't need to enter leading zeros.)	✓	✓	✓	✓
`Description`		✓		✓
`Subject`	✓	✓		✓
`Web Company` (of person who submitted the case online)	✓	✓		✓
`Web Email` (of person who submitted the case online)	✓	✓		✓
`Web Name` (of person who submitted the case online)	✓	✓		✓
`Web Phone` (of person who submitted the case online)	✓	✓		✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓		✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓		✓

Searchable Fields: Channel Program

EDITIONS

Available in: Salesforce Classic

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

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
Description	✓	✓			✓
Name	✓	✓	✓		✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)					✓
All custom fields of type text, text area, long text area, rich text area, email, and phone					✓

Searchable Fields: Channel Program Level

EDITIONS

Available in: Salesforce Classic

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

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
Channel Program Level	✓	✓			✓
All custom auto-number fields and					✓

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
custom fields that are set as an external ID (You don't need to enter leading zeros.)					
All custom fields of type text, text area, long text area, rich text area, email, and phone					✓

Searchable Fields: Chatter Feed

To find information in a feed, use global search or feed search. Neither sidebar search nor advanced search are designed to find information in Chatter feeds.

Note: Global search and feed search return matches for file or link names shared in posts, but not in comments.

Searchable Fields	Sidebar Search	Advanced Search	Global Search	Feed Search
@*Name* (where *Name* is a username)			✓	✓
Comment Body			✓	✓
Commenter Name			✓	✓
File Name			✓	✓
Group Name			✓	✓
Links			✓	✓
Origin of Post (Group, Person, or Record Name			✓	✓
Post Body			✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Chatter Group

Neither sidebar search nor advanced search are designed to find Chatter groups. To find a Chatter group, use global search or the search tools on the Groups tab. Global search results include archived groups.

Searchable Fields	Sidebar Search	Advanced Search	Global Search	Groups Tab
`Description`			✓	✓
`Group Name`			✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Coaching

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Name`	✓	✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓	✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Community

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Global Search
`Community Name`			✓	

EDITIONS

Available in: Salesforce Classic

Available in all editions

Searchable Fields: Contact

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
Assistant	✓	✓			✓
Asst. Phone	✓	✓			✓
Department		✓			✓
Description		✓			✓
Email	✓	✓			✓
Fax	✓	✓			✓
First Name	✓	✓	✓	✓	✓
First Name (Local)	✓	✓	✓	✓	✓
Home Phone	✓	✓			✓
Last Name	✓	✓	✓	✓	✓
Last Name (Local)	✓	✓	✓	✓	✓
Mailing Address		✓			✓
Middle Name	✓	✓		✓	✓
Middle Name (Local)	✓	✓		✓	✓
Mobile	✓	✓			✓
Other Address		✓			✓
Other Phone	✓	✓			✓

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
`Phone`	✓	✓			✓
`Suffix`	✓	✓		✓	✓
`Title`		✓			✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓			✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓			✓

Searchable Fields: Salesforce CRM Content

EDITIONS

Available in: Salesforce Classic

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

Neither sidebar search nor advanced search are designed to find content. To find content, use global search (results appear as files) or the search tools on the Content tab.

Searchable Fields	Sidebar Search	Advanced Search	Global Search	Content Tab
`Body`			✓	✓
`Description`			✓	✓
`File`			✓	✓
`Owner`			✓	✓
`Title`			✓	✓
`Version`			✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)			✓	✓

Searchable Fields	Sidebar Search	Advanced Search	Global Search	Content Tab
All custom fields of type text, text area, long text area, rich text area, email, and phone			✓	✓

Searchable Fields: Contract

EDITIONS

Available in: Salesforce Classic

Available in: **Performance** and **Developer** Editions

Available in: **Professional**, **Enterprise**, and **Unlimited** Editions with the Sales Cloud

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Global Search
`Billing Address`		✓		✓
`Contract Name`	✓	✓	✓	✓
`Contract Number`	✓	✓	✓	✓
`Description`		✓		✓
`Shipping Address`		✓		✓
`Special Terms`		✓		✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓		✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓		✓

Searchable Fields: Contract Line Item

EDITIONS

Available in: Salesforce Classic

Available in: **Performance** and **Developer** Editions

Available in: **Professional**, **Enterprise**, and **Unlimited** Editions with the Sales Cloud

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Description`		✓	✓
`Name`	✓	✓	✓

Searchable Fields: Custom Object

EDITIONS

Available in: Salesforce Classic

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

Custom object records are searchable in the Salesforce user interface only if the custom object is associated with a custom tab. Users aren't required to add the tab for display. By default, search is disabled for new custom objects. Admins enable **Allow Search** when setting up new custom objects.

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
`Name`	✓	✓	✓	✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓			✓
All custom fields of type email and phone	✓	✓			✓
All custom fields of type text, text area, long text area,		✓			✓

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
and rich text area					

Searchable Fields: D&B Company

To have access to D&B Company records, your organization must have Data.com Prospector or Data.com Clean.

EDITIONS

Available in: Salesforce Classic

Available with a Data.com Prospector license in: **Contact Manager** (no Lead object), **Group**, **Professional**, **Enterprise**, **Performance**, and **Unlimited** Editions

Searchable Fields	Sidebar Search	Advanced Search	Global Search
Company City		✓	✓
Company Country		✓	✓
Company Description		✓	✓
D-U-N-S Number		✓	✓
Facsimile Number	✓	✓	✓
Mailing Address		✓	✓
Primary Address		✓	✓
Primary Business Name	✓	✓	✓
Telephone Number	✓	✓	✓
Ticker Symbol		✓	✓
URL		✓	✓

Searchable Fields: Discussion

Discussions support only standard lookup searches.

EDITIONS

Available in: Salesforce Classic

Available in all editions

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Global Search
Title			✓	

Searchable Fields: Document

To find a document, use global search or the **Find Document** button on the Documents tab. Neither sidebar search nor advanced search are designed to find documents.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Global Search	Documents Tab
`Document Name`			✓	✓	✓
`Body`				✓	✓
`Keywords`			✓	✓	✓
All standard text fields				✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)				✓	✓
All custom fields of type text, text area, long text area, rich text area, email, and phone				✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Entitlement

Searchable Fields	Sidebar Search	Standard Lookup	Exhanced Lookup	Advanced Search	Global Search
`Entitlement Name`	✓	✓		✓	✓
All custom auto-number fields and custom fields that are set as an external ID	✓			✓	✓

EDITIONS

Available in: Salesforce Classic

Available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** editions with the Service Cloud

Searchable Fields	Sidebar Search	Standard Lookup	Exhanced Lookup	Advanced Search	Global Search
(You don't need to enter leading zeros.)					
All custom fields of type text, text area, long text area, rich text area, email, and phone				✓	✓

Searchable Fields: External Object

An external object accesses data that's stored outside your Salesforce org. Your Salesforce admin controls which external objects are searchable. Which external object fields are searched depends on how the external system handles searches. If the search results aren't as you expected, use case-sensitive search strings that contain only alphanumeric characters. If the results still aren't as expected, contact your admin for recommendations on searching your specific external system.

Note:

- Lookup search isn't available for external lookup relationship fields. To edit an external lookup relationship field, manually enter the value of the `External ID` standard field for the parent record. This limitation doesn't apply when the parent external object is associated with the cross-org adapter for Salesforce Connect.
- Lookup search isn't available for indirect lookup relationship fields. To edit an indirect lookup relationship field, manually enter the value of the target field of the parent record. The target field is the custom field with `External ID` and `Unique` attributes that was selected when the indirect lookup relationship was created. To determine related records, Salesforce matches target field values against the values of the indirect lookup relationship field on the child object.

Searchable Fields	Sidebar Search	Advanced Search	Global Search
Text, text area, and long text area fields			✓

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Salesforce Connect is available in: **Developer** Edition and for an extra cost in: **Enterprise**, **Performance**, and **Unlimited** Editions

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

Federated Search is available in: **Enterprise**, **Professional**, **Unlimited**, and **Developer** Editions

Searchable Fields: File

Neither sidebar search nor advanced search are designed to find files. To find a file, use global search or the search tools on the Files tab.

Searchable Fields	Sidebar Search	Advanced Search	Global Search	Files Tab
`Body`			✓	✓
`Description`			✓	✓
`Extension` (such as ppt)			✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields	Sidebar Search	Advanced Search	Global Search	Files Tab
`Name`			✓	✓
`Owner`			✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)			✓	✓
All custom fields of type text, text area, long text area, rich text area, email, and phone			✓	✓

Searchable Fields: Goal

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Description`		✓	✓
`Goal Name`	✓	✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓	✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓	✓

Searchable Fields: Idea

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Global Search
`Idea Body`		✓		✓
`Description`		✓		✓
`Title`	✓	✓	✓	✓

Searchable Fields: Knowledge Article

Neither sidebar search nor advanced search is designed to find articles. To find an article, use global search or the search tools in the sidebar on the Articles tab.

Searchable Fields	Sidebar Search	Advanced Search	Global Search	Articles Tab
All standard text fields			✓	✓
`Body`			✓	✓
`File`			✓	✓
`Summary`			✓	✓
`Title`			✓	✓
`URL`			✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)			✓	✓
All custom fields of type text, text area, long text area, rich text area, email, and phone			✓	✓

EDITIONS

Salesforce Knowledge is available in: Salesforce Classic.

Salesforce Knowledge is available in: **Performance** and **Developer** Editions and in **Unlimited** Edition with the Service Cloud.

Salesforce Knowledge is available for an additional cost in: **Enterprise** and **Unlimited** Editions.

Searchable Fields: Lead

Note: Once converted, a lead record is no longer searchable, unless your admin has assigned you the "View and Edit Converted Leads" permission. The new account, contact, or opportunity record created from the converted lead is searchable.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Global Search
`Address`		✓		✓
`Company`	✓	✓	✓	✓
`Company D-U-N-S Number`		✓		✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Global Search
`Company Name(Local)`	✓	✓	✓	✓
`Description`		✓		✓
`Email`	✓	✓		✓
`Fax`	✓	✓		✓
`First Name`	✓	✓	✓	✓
`First Name (Local)`	✓	✓	✓	✓
`Last Name`	✓	✓	✓	✓
`Last Name (Local)`	✓	✓	✓	✓
`Middle Name`	✓	✓		✓
`Mobile`	✓	✓		✓
`Phone`	✓	✓		✓
`Suffix`	✓	✓		✓
`Title`		✓		✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓		✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓		✓

Searchable Fields: Live Chat Transcript

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Body`		✓	✓
`Supervisor Transcript Body`		✓	✓

EDITIONS

Available in: Salesforce Classic

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** editions

Searchable Fields: Macro

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Description`		✓	✓
`Name`	✓	✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Metric

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Description`		✓	✓
`Metric Name`	✓	✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓	✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Note

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Body`		✓	✓
`Title`	✓	✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Operating Hours

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
Description		✓		✓	✓
Name	✓	✓	✓	✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)					✓
All custom fields of type text, text area, long text area, rich text area, email, and phone					✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Opportunity

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
Description		✓			✓
Opportunity Name	✓	✓	✓	✓	✓
Account Name			✓		

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓			✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓			✓

Searchable Fields: Order

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Billing Address`		✓	✓
`Description`		✓	✓
`Order Name`	✓	✓	✓
`Order Number`	✓	✓	✓
`Order Reference Number`		✓	✓
`PO Number`		✓	✓
`Shipping Address`		✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓	✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓	✓

EDITIONS

Available in: Salesforce Classic

Orders are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Searchable Fields: Partner Fund Allocation

EDITIONS

Available in: Salesforce Classic

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

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
Description	✓	✓			✓
Name	✓	✓	✓		✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)					✓
All custom fields of type text, text area, long text area, rich text area, email, and phone					✓

Searchable Fields: Partner Fund Claim

EDITIONS

Available in: Salesforce Classic

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

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
Partner Fund Claim	✓	✓			✓
All custom auto-number fields and custom fields					✓

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
that are set as an external ID (You don't need to enter leading zeros.)					
All custom fields of type text, text area, long text area, rich text area, email, and phone					✓

Searchable Fields: Partner Fund Request

EDITIONS

Available in: Salesforce Classic

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

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
Description	✓	✓			✓
Desired Outcome	✓	✓			✓
Name	✓	✓	✓		✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)					✓
All custom fields of type text, text area, long text area, rich text area, email, and phone					✓

Searchable Fields: Partner Marketing Budget

EDITIONS

Available in: Salesforce Classic

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

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
Description	✓	✓			✓
Name	✓	✓	✓		✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)					✓
All custom fields of type text, text area, long text area, rich text area, email, and phone					✓

Searchable Fields: People

EDITIONS

Available in: Salesforce Classic

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

Neither sidebar search nor advanced search are designed to find people; however, sidebar search and advanced search can be used to find users. See Searchable Fields: User.

To find people, use global search or the search tools on the People tab.

Searchable Fields	Sidebar Search	Advanced Search	Global Search	People Tab
`About Me`			✓	
`Address`			✓	
`Email`			✓	
`First Name`			✓	✓
`Last Name`			✓	✓

Searchable Fields	Sidebar Search	Advanced Search	Global Search	People Tab
`Name`			✓	✓
`Nickname`			✓	✓
`Phone`			✓	
`Record ID` (15 character Record ID only)			✓	
`Title`			✓	
`Username`			✓	
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)			✓	
All custom fields of type text, text area, long text area, rich text area, email, and phone			✓	

Note: Information in hidden fields on a profile is not searchable by other partners and customers in the community, but is searchable by users in the company's internal organization.

Searchable Fields: Performance Cycle

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Name`	✓	✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓	✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓	✓

Searchable Fields: Person Account

Note: The Person Account object contains fields that originate from both the Business Account and Contact objects. All search terms are compared to all searchable business account and contact fields at the same time.

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
Account Name	✓	✓	✓	✓	✓
Account Name (Local)	✓	✓	✓	✓	✓
Account Number	✓	✓			✓
Account Site	✓	✓			✓
Assistant	✓	✓			✓
Assistant Phone	✓	✓			✓
Billing Address		✓			✓
Description		✓			✓
Email	✓	✓			✓
Fax	✓	✓			✓
Home Phone	✓	✓			✓
Mailing Address		✓			✓
Mobile	✓	✓			✓
Other Address		✓			✓
Other Phone	✓	✓			✓

EDITIONS

Available in: Salesforce Classic

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

The available person account fields vary according to which Salesforce edition you have.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
Shipping Address		✓			✓
Ticker Symbol	✓	✓			✓
Title		✓			✓
Website	✓	✓		✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓			✓
All account and contact custom fields of type text, text area, long text area, rich text area, email, and phone		✓			✓

Searchable Fields: Price Book

Neither global search, sidebar search, nor advanced search are designed to find price books. To find a price book, use the **Price Books** area on the Products tab.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Global Search	Products Tab Search
Price Book Description					✓
Price Book Name			✓		✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Product

EDITIONS

Available in: Salesforce Classic

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

Neither sidebar search nor advanced search are designed to find price books or products. To find a product, use global search or the **Find Products** area on the Products tab.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Global Search	Products Tab Search
`Product Code`			✓	✓	✓
`Product Description`				✓	✓
`Product Name`			✓	✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)				✓	✓
All custom fields of type text, text area, long text area, rich text area, email, and phone				✓	✓

Searchable Fields: Question

EDITIONS

Available in: Salesforce Classic

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** editions

The Answers tab in Salesforce lists all the questions posted to an answers community.

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Question Body`		✓	✓
`Question Title`	✓	✓	✓
`Reply Body`		✓	✓

Searchable Fields: Quick Text

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Message`		✓	✓
`Name`	✓	✓	✓

EDITIONS

Available in: Salesforce Classic

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** editions

Searchable Fields: Quote

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup	Global Search
`Quote Name`	✓	✓	✓	✓
`Quote Number`	✓	✓		✓
All custom fields of type text, text area, long text area, rich text area, email, and phone				✓

EDITIONS

Available in: Salesforce Classic

Quotes available in: **Performance** and **Developer** Editions and in **Professional**, **Enterprise**, and **Unlimited** Editions with the Sales Cloud

Searchable Fields: Report

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Description`	✓	✓	✓
`Report Name`	✓	✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Resource Absence

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
`Absence Number`	✓	✓		✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
`Description`		✓		✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)					✓
All custom fields of type text, text area, long text area, rich text area, email, and phone					✓

Searchable Fields: Reward Fund

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Name`	✓	✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓	✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Reward Fund Type

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Name`	✓	✓	✓
All custom auto-number fields and custom fields that are set as an external ID	✓	✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields	Sidebar Search	Advanced Search	Global Search
(You don't need to enter leading zeros.)			
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓	✓

Searchable Fields: Self-Service User

Self-service users support only standard lookup searches.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Global Search
`First Name`			✓	
`Last Name`			✓	

EDITIONS

Available in: Salesforce Classic

Available in all editions

Searchable Fields: Service Appointment

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
`Appointment Number`	✓	✓		✓	✓
`Description`		✓		✓	✓
`Subject`		✓		✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)					✓
All custom fields of type text, text area,					✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
long text area, rich text area, email, and phone					

Searchable Fields: Service Contract

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Contract Number`	✓	✓	✓
`Description`		✓	✓
`Contract Name`	✓	✓	✓
`Special Terms`		✓	✓

EDITIONS

Available in both: Salesforce Classic and Lightning Experience

Available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions with the Service Cloud

Searchable Fields: Service Crew

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
Name	✓	✓	✓		✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)					✓
All custom fields of type text, text area, long text area, rich text area,					✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
email, and phone					

Searchable Fields: Service Crew Member

EDITIONS

Available in: Salesforce Classic

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

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
Name	✓	✓	✓		✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)					✓
All custom fields of type text, text area, long text area, rich text area, email, and phone					✓

Searchable Fields: Service Resource

EDITIONS

Available in: Salesforce Classic

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

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
`Description`		✓		✓	✓
`Name`	✓	✓	✓	✓	✓

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)					✓
All custom fields of type text, text area, long text area, rich text area, email, and phone					✓

Searchable Fields: Service Resource Skill

EDITIONS

Available in: Salesforce Classic

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

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
`Resource Skill Number`	✓	✓		✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)					✓
All custom fields of type text, text area, long text area, rich text area, email, and phone					✓

Searchable Fields: Service Territory

EDITIONS

Available in: Salesforce Classic

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

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
`Description`		✓		✓	✓
`Name`	✓	✓	✓	✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)					✓
All custom fields of type text, text area, long text area, rich text area, email, and phone					✓

Searchable Fields: Service Territory Member

EDITIONS

Available in: Salesforce Classic

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

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
`Member Number`				✓	✓
All custom auto-number fields and custom fields					✓

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
that are set as an external ID (You don't need to enter leading zeros.)					
All custom fields of type text, text area, long text area, rich text area, email, and phone					✓

Searchable Fields: Skill

Note: Lightning Experience users can see skills endorsements that they've received in the feed.

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Skill Name`	✓	✓	✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓	✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Solution

Neither sidebar search nor advanced search are designed to find solutions. To find a solution, use global search or the **Find Solution** button on the Solutions tab.

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Thanks Badge

Note: Lightning Experience users can see thanks badges that they've received in the feed.

EDITIONS

Available in: Salesforce Classic

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

Badge

The attributes of a type of thanks badge, such as the badge name, description, and image.

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Badge Name`	✓	✓	✓
`Description`		✓	✓

Badge Received

A specific thanks badge that is given to a user.

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Badge Received Name`	✓	✓	✓
`Description`		✓	✓

Searchable Fields: Topic

Neither sidebar search nor advanced search are designed to find topics. To find a topic, use global search.

EDITIONS

Available in: Salesforce Classic

Available in all editions

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Description`		✓	✓
`Topic Name`	✓	✓	✓

Searchable Fields: User

Note: If you're using Chatter and searching for people, see Searchable Fields: People.

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
`About Me`		✓			✓
`Address`	✓	✓			✓

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
`Email`	✓	✓			✓
`First Name`	✓	✓	✓	✓	✓
`Last Name`	✓	✓	✓		✓
`Middle Name`	✓	✓		✓	✓
`Name`	✓	✓	✓	✓	✓
`Nickname`	✓	✓		✓	✓
`Phone`	✓	✓			✓
`Record ID` (15 character Record ID only)	✓	✓			✓
`Suffix`	✓	✓		✓	✓
`Title`	✓	✓			✓
`Username`	✓	✓			✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓			✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓			✓

Searchable Fields: Work.com Feedback

Note: To have access to the following objects, your org must have the Work.com add-on.

Feedback

A response to a feedback question or request.

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Feedback Name`	✓	✓	✓

EDITIONS

Available in: Salesforce Classic

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

Feedback Question

A free-form text question or multiple choice question within a larger set of questions.

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Feedback Question Name`	✓	✓	✓
`Instruction Detail`		✓	✓

Feedback Question Set

A set of questions being asked in a performance cycle.

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Feedback Question Set Name`	✓	✓	✓

Feedback Request

A one-time feedback request on a subject or topic.

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Feedback Request Name`	✓	✓	✓

Searchable Fields: Work Order

EDITIONS

Available in: Salesforce Classic

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

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
`Description`		✓	✓	✓	✓
`Subject`		✓	✓	✓	✓
`Work Order Number`	✓	✓			✓
All custom auto-number fields and custom fields	✓	✓			✓

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
that are set as an external ID (You don't need to enter leading zeros.)					
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓			✓

Searchable Fields: Work Order Line Item

Note: If available, there is an option when using enhanced lookup search to query all searchable fields, not just the fields checked in the Enhanced Lookup Search (Default) column in the table.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search (Default)	Global Search
`Description`		✓	✓	✓	✓
`Work Order Line Item Number`	✓	✓			✓
All custom auto-number fields and custom fields that are set as an external ID (You don't need to enter leading zeros.)	✓	✓			✓
All custom fields of type text, text area, long text area, rich text area, email, and phone		✓			✓

EDITIONS

Available in: Salesforce Classic

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

Configure Lookup Search

Choose which columns appear to users in the lookup search results.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

IN THIS SECTION:

Configure Lookup Search in Salesforce Classic

Enable enhanced lookups and lookup auto-completion and customize lookup filter fields.

Configure Lookup Search in Lightning Experience

Customize which columns appear to users in the lookup dialog search results using the Search Results search layout customization setting. Users aren't able to filter using these columns. They are intended to provide contextual help for determining which record to associate.

Configure Lookup Search in Salesforce Classic

Enable enhanced lookups and lookup auto-completion and customize lookup filter fields.

EDITIONS

Available in: Salesforce Classic

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

IN THIS SECTION:

Enable Enhanced Lookups

Enable enhanced lookups so users can sort, filter, and page through their results. Enhanced lookups are available only for specific objects.

Specify Lookup Search Filter Fields

After enabling enhanced lookups, specify which fields users can use to filter lookup search results. If you don't specify any fields, your users can't use filters in enhanced lookup dialogs. Enhanced lookups are available only for specific objects.

Enable Lookup Auto-Completion

Enable lookup auto-completion so users can select items from a dynamic list of matching, recently used records when editing a lookup field. It's supported for account, contact, user, opportunity, and custom object lookups.

Enable Enhanced Lookups

Enable enhanced lookups so users can sort, filter, and page through their results. Enhanced lookups are available only for specific objects.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To enable enhanced lookups:

- Customize Application

Note: Custom object records are searchable in the Salesforce user interface only if the custom object is associated with a custom tab. Users aren't required to add the tab for display.

1. From Setup, enter `Search Settings` in the Quick Find box, then select **Search Settings**.
2. In the Lookup Settings area, select the objects for which you want to enable enhanced lookup functionality.
3. Click **Save**.

After enabling enhanced lookups, specify which fields users can use to filter lookup search results. If you don't specify any fields, your users can't use filters in enhanced lookup dialogs. Fields configured to use enhanced lookups don't support single character searches (except for searches in Chinese, Japanese, Korean, and Thai) or wildcards at the beginning of search terms.

Note: If you enable enhanced lookups in your org, it is also enabled for the Visualforce pages you create. However, enhanced fields aren't available for Force.com sites.

SEE ALSO:

Configure Lookup Search in Salesforce Classic

Specify Lookup Search Filter Fields

After enabling enhanced lookups, specify which fields users can use to filter lookup search results. If you don't specify any fields, your users can't use filters in enhanced lookup dialogs. Enhanced lookups are available only for specific objects.

1. From the management settings for an object, go to **Search Layouts**.
2. For the Lookup Filter Fields layout, click **Edit**.
3. Use the arrows to add or remove fields from the layout and to define the order in which the fields display. You can add up to six filter fields to the Selected Fields list. To select more than one field, use CTRL+click, or SHIFT+click to select multiple items in a range.
4. Click **Save**.

Note: If you enable enhanced lookups in your org, it is also enabled for the Visualforce pages you create. However, enhanced fields aren't available for Force.com sites.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To specify lookup filter fields:
- Customize Application

SEE ALSO:

Configure Lookup Search in Salesforce Classic

Find Object Management Settings

Enable Lookup Auto-Completion

Enable lookup auto-completion so users can select items from a dynamic list of matching, recently used records when editing a lookup field. It's supported for account, contact, user, opportunity, and custom object lookups.

1. From Setup, enter `Search Settings` in the `Quick Find` box, then select **Search Settings**.
2. In the Search Settings area, select the object lookups for which you want to enable auto-completion. Currently, only account, contact, opportunity, user, and custom object lookups can use this feature.
3. Click **Save**.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To enable lookup auto-completion:
- Customize Application

To use lookup auto-completion:
- Edit on the record that includes the lookup field

SEE ALSO:

Configure Lookup Search in Salesforce Classic

Configure Lookup Search in Lightning Experience

Customize which columns appear to users in the lookup dialog search results using the Search Results search layout customization setting. Users aren't able to filter using these columns. They are intended to provide contextual help for determining which record to associate.

In Lightning Experience, use **Search Results** under the **Search Layouts** customization setting to change which fields appear in the search results for both global search and lookup search. You aren't required to separately update **Lookup Dialogs**.

The order of fields in the search layout also affects the secondary field displayed in Lightning Experience instant results. The second usable field as chosen in this step appears as the secondary field in instant results.

- Examples of **usable** fields are short-text, phone, currency, percent, date, or time fields.
- Examples of **unusable** fields are HTML-formatted fields (URL and email), inline image fields, pick lists, or long-text fields.

EDITIONS

Available in: Lightning Experience

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

USER PERMISSIONS

To specify lookup filter fields:

- Customize Application

SEE ALSO:

Find Object Management Settings in Lightning Experience

Configure Synonym Groups

A search for one term in a synonym group returns results for all terms in the group. For example, a search for *USB drive* returns results for all terms in the synonym group, which contains *USB drive*, *thumb drive*, *flash stick*, and *memory stick*. Synonym groups remove the guesswork for users searching for records.

These objects are supported.

- Case
- Chatter Feed
- File
- Knowledge Article
- Idea
- Question
- Service Appointment
- Service Resource
- Service Territory
- Work Order
- Work Order Line Item

EDITIONS

Available in: both Lightning Experience and Salesforce Classic

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

1. From Setup, enter `Synonyms` in the Quick Find box, then select **Synonyms**.
2. To create a synonym group, click **New** in the Custom Synonym Groups section. You can create up to 10,000 synonym groups with up to six terms in each group.

Configure Search Settings in Salesforce Classic

Enable document content search, CJKT search optimization, sidebar search auto-complete, and more. Configure the lookup settings and the number of search results per object and lookup settings.

To change your org's search settings, enter `Search Settings` in the **Quick Find** box, then select **Search Settings**.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To modify search settings:

- Customize Application

Search Settings

Field	Description
Enable "Limit to Items I Own" Search Checkbox	If this setting is enabled, the **Limit to Items I Own** option is available to users. The option allows users to include only records for which they are the record owner when entering search queries in the sidebar. Note: The **Limit to Items I Own** option that appears in advanced search is always available to users, regardless of this setting.
Enable Document Content Search	If this setting is enabled, users can perform a full-text document search. When a new document is uploaded or an old one is replaced, its contents are available as search terms to retrieve the document. This setting applies only to searches for the document object.
Enable Search Optimization if your Content is Mostly in Japanese, Chinese, or Korean	If this setting is enabled, search is optimized for the Chinese, Japanese, and Korean languages in the sidebar search. It affects sidebar search and the account search for **Find Duplicates** on a lead record in sidebar search and global search. Note: Enable this option only if users are searching mostly in Chinese, Japanese, or Korean, and if the text in searchable fields is mostly in those languages. Don't enable this option if you expect content and searches to be mostly in other languages.
Use Recently Viewed User Records for Blank and Auto-Complete Lookups	If this setting is enabled, the list of records that are returned from a user auto-complete lookup and from a blank user lookup is taken from the user's recently viewed user records. This setting applies only to lookups in the *user* object.

Field	Description
	If this setting isn't enabled, the dialog box shows a list of recently accessed user records from across the org.
Enable English-Only Spell Correction for Knowledge Search	If this setting is enabled, search returns results for corrected spellings of English search terms: • On the Articles and Article Management tabs • In the articles tool in Case Feed • In the Salesforce Knowledge sidebar in the Salesforce console
Enable Drop-Down List for Sidebar Search	If this setting is enabled, a drop-down appears for users to choose whether to search within tags, within a specific object, or across all objects.
Enable Sidebar Search Auto-Complete	If this setting is enabled, when users start typing search terms, sidebar search displays a matching list of recently viewed records.
Enable Single-Search-Result Shortcut for Sidebar and Advanced Search	If this setting is enabled, users skip the search results page and go directly to the record's detail page when their search returns only a single item. Note: This setting doesn't apply to tags, case comments (in advanced search), and global search. If the search result is a single tag, case comment, or item in global search, the search results page still appears.
Number of Search Results Displayed Per Object	The Number of Search Results Displayed Per Object area allows you to configure the number of items that are returned for each object in the Search Results page.
Lookup Settings	The Lookup Settings area allows you to enable enhanced lookups and lookup auto-completion for enhanced lookup-enabled objects and any custom object lookups.

SEE ALSO:

Make Search Faster

Configure Search Results Filters in Salesforce Classic

Admins choose the filters available to users for refining search results. Choosing the correct filters for each object is important so that users can easily navigate through search results to find the right record.

1. On the Search Results page, in an object's related list, select **Customize** > **Filters for All Users**.

   Alternatively, from the management settings for an object, go to Search Layouts, and click **Edit** for **Search Filter Fields**.

2. To choose columns, use **Add** and **Remove**.
3. To reorder columns, use **Up** and **Down**.
4. Click **Save**.

Note: Search result filters defined for an object in the internal org also apply for search results for that object in communities.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To change search layouts:
- Customize Application

SEE ALSO:

Find Object Management Settings

Set Up and Manage Federated Search

Do your users search for content stored outside of Salesforce? Federated search makes it easy to add external search engines (or connectors) to your org. Users look for information using Salesforce global search and see external results in a single search results page. Understand more about how federated search works, how to set it up, and how users see results.

EDITIONS

Available in: both Lightning Experience and Salesforce Classic

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

IN THIS SECTION:

Search for Data from External Search Providers

With federated search, users can search data stored in repositories outside of Salesforce while remaining inside the Salesforce user interface. For example, a team member can use Salesforce global search and see results from external search engines. Salesforce has also partnered with Coveo, Docurated, and Swiftype to make it easy to connect external search providers to Salesforce. Leveraging these partner's services, you can search through the external repositories they serve. For example, Dropbox, Confluence, SharePoint.

Configure a Solr Server to Support OpenSearch

If you want Solr search results to appear as external results in Salesforce, configure the server to support OpenSearch and Atom XML format. The OpenSearch standard is the basis for Salesforce Federated Search, which displays external search results in Salesforce. Configure your Solr server before creating an external data source in Salesforce.

Define an External Data Source for Federated Search: OpenSearch

Let users search in your Salesforce org and access data from an external search provider.

Considerations for Federated Search

When setting up federated search, familiarize yourself with the nice-to-knows and limitations.

How Results from External Search Providers Appear to Users

Understand how users see and interact with external search results in both Salesforce Classic and Lightning Experience.

Search for Data from External Search Providers

EDITIONS

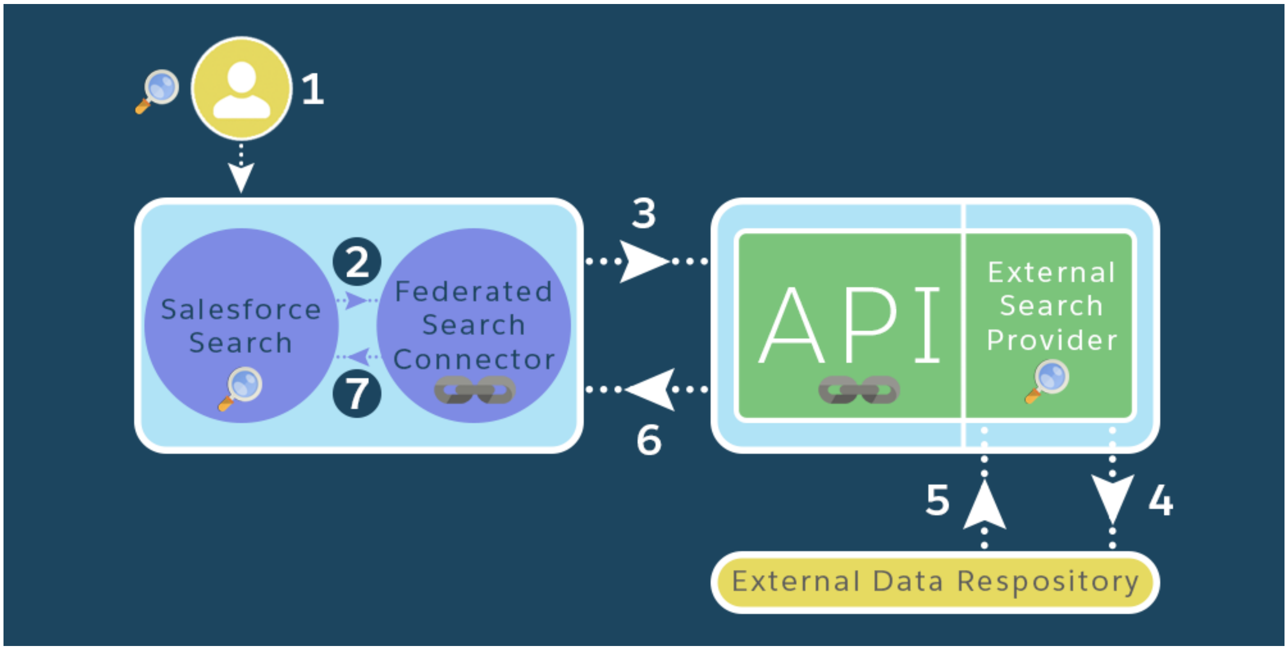
Available in: both Lightning Experience and Salesforce Classic

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

With federated search, users can search data stored in repositories outside of Salesforce while remaining inside the Salesforce user interface. For example, a team member can use Salesforce global search and see results from external search engines. Salesforce has also partnered with Coveo, Docurated, and Swiftype to make it easy to connect external search providers to Salesforce. Leveraging these partner's services, you can search through the external repositories they serve. For example, Dropbox, Confluence, SharePoint.

The federated search connector runs search requests within Salesforce and connects to an external provider with the Salesforce Federated Search API, which is based on the OpenSearch standard. The search results are then displayed to users in Salesforce.

1. In the Salesforce user interface, an end user searches for a record that is stored outside of Salesforce.
2. Salesforce search sends the request to the federated search connector.
3. The federated search connector sends a request to the external search provider conforming to the Salesforce Federated Search API.
4. The external search provider searches the external data repository index (like DropBox).
5. The external search provider gets results from the external data repository index.
6. The external search provider returns the results to the federated search connector.
7. The federated search connector returns the results in a Salesforce search results page.



Configure a Solr Server to Support OpenSearch

If you want Solr search results to appear as external results in Salesforce, configure the server to support OpenSearch and Atom XML format. The OpenSearch standard is the basis for Salesforce Federated Search, which displays external search results in Salesforce. Configure your Solr server before creating an external data source in Salesforce.

EDITIONS

Available in: both Lightning Experience and Salesforce Classic

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

IN THIS SECTION:

1. Create the Atom XSL File

   To transform the Solr default search results from JSON to XML Atom, you create an XSL file. Solr provides example files that you can customize for your server.

2. Edit and Test the Solr Query

   Add parameters that reference the Atom XSL file to the Solr query. Then test your changes to make sure that results are appearing in XML Atom format.

3. Publish the OpenSearch Description

   To transform the Solr default search results from JSON to XML Atom, create and publish an OpenSearch description file. This XML file defines the search query URL and supported parameters.

Create the Atom XSL File

To transform the Solr default search results from JSON to XML Atom, you create an XSL file. Solr provides example files that you can customize for your server.

1. Find a sample Atom XSL file from the Solr distribution at solr.6.5.1/server/solr/configsets/sample_techproducts_configs/xslt/example_atom.xsl.
2. Save the file in the xslt folder that has the example xsl file.
3. In the `entry` section, edit the `name`, `features`, and `timestamp` names of the `title`, `summary`, and `updated` fields, respectively. This section transforms the search results into Atom. When changing the names, review the example XML files in the `solr.6.5.1/example/exampledocs` folder created when Solr was installed. Or run a search against Solr, and review the JSON search results.

Example: Here's an example of an Atom XSL file.

```
<!-- search results xslt -->
 <xsl:template match="doc">
   <xsl:variable name="id" select="str[@name='id']"/>
   <entry>
     <title><xsl:value-of select="str[@name='name']"/></title>
     <link href="http://localhost:8983/solr/select?q={$id}"/>
     <id>tag:localhost,2007:<xsl:value-of select="$id"/></id>
     <summary><xsl:value-of select="arr[@name='features']"/></summary>
     <updated><xsl:value-of select="date[@name='timestamp']"/></updated>
   </entry>
 </xsl:template>
```

Edit and Test the Solr Query

Add parameters that reference the Atom XSL file to the Solr query. Then test your changes to make sure that results are appearing in XML Atom format.

1. Add these parameters to the Solr query: `wt=xslt` and `tr=`*`file_name`*`.xsl`, where *file_name* is the name of your Atom XSL file. For example, `tr=acme.xsl`.
2. Use this URL to test your query: http://localhost:8983/solr/techproducts/select?q=sd500&wt=xslt&tr=example_atom.xsl. In this test, the core name is *techproducts* and the search term is *sd500*.

Example: Here's an example of a response formatted in Atom XML.

```
<feed xmlns="http://www.w3.org/2005/Atom">
   <title>Example Solr Atom 1.0 Feed</title>
   <subtitle>
     This has been formatted by the sample "example_atom.xsl" transform - use your own
 XSLT to get a nicer Atom feed.
   </subtitle>
   <author>
     <name>Apache Solr</name>
     <email>solr-user@lucene.apache.org</email>
   </author>
   <link rel="self" type="application/atom+xml"
href="http://localhost:8983/solr/q=sd500&wt=xslt&tr=atom.xsl"/>
   <updated/>
   <id>tag:localhost,2007:example</id>
   <entry>
     <title>Canon PowerShot SD500</title>
     <link href="http://localhost:8983/solr/select?q=9885A004"/>
     <id>tag:localhost,2007:9885A004</id>
     <summary>
       3x zoop, 7.1 megapixel Digital ELPHmovie clips up to 640x480 @30 fps2.0" TFT
LCD, 118,000 pixelsbuilt in flash, red-eye reduction
     </summary>
   <updated/>
   </entry>
</feed>
```

Publish the OpenSearch Description

To transform the Solr default search results from JSON to XML Atom, create and publish an OpenSearch description file. This XML file defines the search query URL and supported parameters.

1. To create an OpenSearch description XML file, see OpenSearch URL template syntax. The query host, core name, and XSL file name are required.
2. Publish the XML file either with an HTTP file server or file sharing service. To publish via Google Drive:
   a. Put the OpenSearch description XML file in a GDrive folder.
   b. Set the share settings to make the file publicly visible.
   c. Determine the file direct-link URL using the Google Drive Direct-Link Generator.
3. Note the URL to the published XML file. Use this URL when creating the OpenSearch external data source within Salesforce. The OpenSearch description is accessed only when creating the OpenSearch external data source or when the data source is synchronized.

Example: This OpenSearch description includes the minimum required.

```
<?xml version="1.0" encoding="UTF-8"?>
<OpenSearchDescription xmlns="http://a9.com/-/spec/opensearch/1.1/">
```

```
  <ShortName>Solr Search</ShortName>
  <Url type="application/atom+xml"
template="http://localhost:8983/solr/techproducts/select?q={searchTerms}&wt=xslt&tr=example_atom.xsl"/>
</OpenSearchDescription>
```

Define an External Data Source for Federated Search: OpenSearch

Let users search in your Salesforce org and access data from an external search provider.

Salesforce has also partnered with Coveo, Docurated, and Swiftype to make it easy to connect external search providers to Salesforce. Leveraging these partner's services, you can search through the external repositories they serve. For example, Dropbox, Confluence, SharePoint. If you use external data sources managed by Coveo, Docurated, or Swiftype, work with them to set up their service as an external search provider.

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

Field	Description
External Data Source	A user-friendly name for the data source that's displayed in the Salesforce user interface.
Name	A unique identifier used to refer to the external data source definition through the API. This field auto-populates with the same name as **External Data Source** when you click in the field.
Type	Select **Federated Search: OpenSearch**.
OpenSearchDescription URL	URL to point to the OpenSearchDescription of the external data source provider. Located in the OpenSearch section of search engine documentation. Include the entire URL, including https://.
Connection Timeout	Number of seconds to wait for a response from the external system before timing out, up to 120 seconds. The default is 20 seconds. Use this field to limit how long to wait for external data to load into your org. Depending on the availability of and the connection to the external system, it can take a long time to retrieve external data.
Search results visible to all profiles	Makes external search results visible to all profiles during the initial setup. If you clear this option or it appears disabled, you can manually set which profiles get search results.

EDITIONS

Available in: both Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To create and edit an external data source:

- Customize Application

Field	Description
Certificate	Associate the authentication certificate to the external data source.
Identity Type	The identity type used to authenticate to the external data source. • If you don't need authentication, select **Anonymous**. • If you need authentication, select **Named Principal**.
Authentication Protocol	The protocol required to access the external data source. • If you selected **Anonymous** for **Identity Type**, select **No Authentication**. • If you selected **Named Principal** for **Identity Type**, select **OAuth 2.0** and complete the additional fields.
Authentication Provider	Look up the name of the OpenID Connect Authentication Provider that you added.
Scope	Autofills to Search.
Start Authentication Flow	Select to start the authentication process.

3. Click **Save**.
4. To ensure that the external data source connects correctly, click **Validate and Sync**.
5. To create the Salesforce external object and a custom field for each table column that's compatible with a Salesforce metadata field type, select the tables and click **Sync**. You can't create an external object manually.

You can customize external objects. Configure the external object label, search result layout, page layout, and field-level security to ensure visibility to individual fields. However, don't change the name of the external object. By default, all fields for the external object are visible to all user profiles. You don't need to create a custom tab for the external object to appear in search results. For Lightning Experience, if you created a custom tab, the source could show up both under External Results and in the list of objects.

Considerations for Federated Search

When setting up federated search, familiarize yourself with the nice-to-knows and limitations.

- By default, all fields for the external object are visible to all user profiles.
- You don't need to create a custom tab for the external object to appear in search results. For Lightning Experience, if you created a custom tab, the source could show up both under External Results and in the list of objects.
- On the search results page, column resizing and text wrapping aren't available for external results.
- In Salesforce Classic, external results appear only in Knowledge sidebar search results.
- Federated Search supports only external lookup relationships, and the Federated Search external object is always the parent.
- Unlike Salesforce Connect, Federated Search external objects only contain fields defined by the external data source. In addition, unlike other external data sources, Federated Search is meant to display search result information, not records.

EDITIONS

Available in: both Lightning Experience and Salesforce Classic

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

How Results from External Search Providers Appear to Users

Understand how users see and interact with external search results in both Salesforce Classic and Lightning Experience.

EDITIONS

Available in: both Lightning Experience and Salesforce Classic

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

Both Lightning Experience and Salesforce Classic

- The external source name on the search results page is the name that was entered when the source was defined.
- External results also appear in console and community search results.
- External results appear in instant results.
- Which fields are searchable, relevance ranking, and any advanced search features (like spell correction) are applied per the external data source. Verify with the external search provider how it searches for content and which special features it offers.
- Salesforce search features (lemmatization, spell correction, nicknames, and synonym group features) and relevance ranking aren't applied to external search results.
- The ability to sort results depends on whether the external search provider supports sorting on certain fields. Options to sort by Relevance and Display URL are always available. However, if the external search provider doesn't support these options, selecting the option doesn't sort results. If the provider supports sorting for other fields, those options appear in the sorting drop-down. Sorting might not be available for all fields.

Salesforce Classic

- External results are included within the list of all searchable objects in alphabetical order.
- The new external source doesn't appear immediately at the top of the search results list because it's new. Users can pin the object to the top of search results by hovering over the object name in the search results object list and clicking the pin icon.

Lightning Experience

- External sources are grouped in the External Results section on the left side, under Search Results.
- The external sources are listed alphabetically. You can't customize the order.
- Frequently used external sources appear in Top Results under Search Results.
- If you added the external data source to the navigation bar, the external source also appears in the Search Results. The source is also listed under Show More in Search Results.
- Users select the Title to go to the record detail page or **View** to go to the external document directly. Depending on the external source, the URL opens in the external source website or in a frame inside Salesforce.

Help Users Find Missing Records

Are users reporting that records aren't appearing in their search results? Admins can troubleshoot common search issues for users. Encouraging users to narrow their search scope or use more specific search terms is always a good first step. Admins can also verify the search status, permissions, and search settings. Learn about search result crowding, also called truncation, and how it affects the results returned.

Have your users tried sorting and filtering results and still can't find a record? Here are some tips for helping them get to the right record faster.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Understand search results crowding or truncation

The search engine applies limits to the number of records analyzed at each stage of the search process. Limits are important because they help maintain performance and don't overwhelm the user with irrelevant records.

Users don't always find all possible matching results because the record that they're looking for falls outside the result limit. This behavior is called crowding or truncation and typically happens when:

- Users have limited permissions or access to records in comparison to the total number of records in the org. These users are considered "low visibility users." Therefore, the records they do have access to might not be part of the results set that is filtered by access permissions. Consider advising users to enter a more specific search term.
- Users search using a term that matches a large number of records. Because the search matches so many records, the search engine can't determine which specific record the user is searching for. This typically happens when the search term isn't specific enough. Consider advising users to enter a more specific search term.
- Users perform a standard lookup search. Lookup searches have additional result limits and only search the record name field. Consider advising users to enter a more specific search term. Admins can also create lookup filters and adjust how lookup search results are displayed.

Encourage users to narrow the search scope

When users first perform a search, they are taken to a results page that lists top results based on the objects they search most frequently. If a certain record is from an object that isn't used frequently, user might not see the record on the first search results page.

If this is the case, users should limit the search scope to the right object. The search is rerun. Potentially, users could see more results, because the full result set limit is applied against a single object.

Encourage users to use more specific search terms

Searches work best when users enter a unique search term. *`Acme Company San Francisco`* returns more relevant results than *`Acme`*.

Review the search layout for user sorting or filtering

Users can sort and filter only the fields that are available as columns on the search results page. Depending on the object type, some fields are more helpful than others. You can choose the available fields for each object in the search layout.

Develop record naming conventions

Although not always possible for existing orgs, encourage users to give their records unique names. This way, searches for the record return fewer results and won't reach the results limit.

Create list views

Create a list view for a specific set of contacts, documents, or other object records that users search for repeatedly. List views have no limits on the number of records and have a set order. Sharing rules are also applied. List views aren't designed to search for a single, specific record. They are meant to search for multiple records by a specific parameter. For example, a list of accounts in your state, leads with a specific lead source, or opportunities above a particular amount.

List views are different from search result filters. Even if global or lookup filters are applied, users can still encounter search crowding. Instead of making more complicated filters, consider countering search crowding with the other tips listed.

Check whether the record's object or field is searchable

Another possible issue is that the record's object or field isn't searchable. Check which fields and objects are searchable.

After a record is created or updated, it can take a few minutes for the new text to be indexed and become searchable. A record doesn't show in the search results until it's in the index. Wait a few minutes and search again. If the record still isn't searchable after 15 minutes, there could be an indexing delay.

Make sure that the object has a tab and that its tab visibility is correct for a user's profile. Custom object records are searchable only if the custom object is associated with a custom tab. Users aren't required to add the tab for display.

Check user permissions and profiles

We show results to users only if they have permission to view them, so records don't appear for users if they don't have access. Users inherit the same access permissions as users below them in the role hierarchy. Check the user permissions, such as org-wide defaults or role hierarchy settings, to make sure that users have the right level of access. You can also manually grant access to your user records so that others can access them. Granting access to a user record makes the user's detail page visible to others. It also makes the user visible in lookups, list views, search, and so on.

Example: Joe Smith, a sales executive at Acme, wants to find the account record for Industrial Computing. He types `Industrial` into the search bar. Because so many records match the search term *Industrial*, a limit is imposed on the results. Unfortunately for Joe, the record he wants is outside the limit. Because Joe used a global search, limits are applied to each object type to make up the record limit. If Joe limited his search to just one object, the limit applies only to that object, increasing the chance that the record he wants is returned. Joe retries by typing `Industrial Computing San Francisco` as a search scoped to just accounts. With a more specific search term and specified object, the search engine returns better matches, even with the same limits applied.

Make Search Faster

Disabling search for custom objects and external objects and scheduling bulk uploads during off-peak hours helps speed up search.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

To make searches faster across your org:

Disable search for custom objects that your users aren't actively searching

Choose which custom objects your users can search by enabling the **Allow Search** setting on the custom object setup page. If you don't need a custom object's records to be searchable, disable search for that custom object. Making a custom object searchable when you don't need your users to find its records slows down searches across your org.

By default, search is disabled for new custom objects. Disabling search doesn't affect reports and list views.

Note: Custom object records are searchable in the Salesforce user interface only if the custom object is associated with a custom tab. Users aren't required to add the tab for display.

Disable search for external objects that your users aren't actively searching

To disable search for an external object, deselect **Allow Search** on its setup page. To include an external object in SOSL and Salesforce searches, enable search on both the external object and the external data source.

By default, search is disabled for new external objects. However, you can validate and sync an external data source to automatically create external objects. Syncing always enables search on the external object when search is enabled on the external data source, and vice versa.

As with custom objects, unnecessarily making an external object searchable can slow down searches across your org.

Avoid making significant changes to your org at once

Creating or updating many records at the same time, such as via data imports, increases the time it takes for each record to become searchable. If you have a large org with many users who frequently make simultaneous updates, schedule bulk uploads and background processes to run during non-peak hours.

Provide Maps and Location Services

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

To generate a map image, an address must include the street and city fields and either the state, postal code, or the country. If an address field is missing any of the required information, a map won't display on the detail page of a record.

The map image on the address is static, but clicking the map image opens Google Maps in a new browser tab on the desktop, and opens a map app on a mobile device.

If your organization has Salesforce offline access enabled, a map doesn't display when a user's device is offline.

To enable your organization's map and location services:

1. From Setup, enter `Maps` in the `Quick Find` box, select **Maps and Location Settings**, then click **Edit**.
2. Check `Enable Maps and Location Services`.
3. Click **Save**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Professional**, **Enterprise**, **Performance**, and **Unlimited** editions.

USER PERMISSIONS

To modify maps and location settings:

- Customize Application

IN THIS SECTION:

Autocomplete on Standard Addresses

When you enable autocomplete on standard addresses, Salesforce app users can enter text on standard address fields and see possible matching addresses in a picklist.

Let Users Select State and Country from Picklists

State and country picklists let users select states and countries from predefined, standardized lists, instead of entering state and country data into text fields. State and country picklists offer faster and easier data entry. They help to ensure cleaner data that can be harnessed for other uses—in reports and dashboards, for example. They protect data integrity by preventing typos, alternate spellings, and junk data—even in records updated through the API.

Autocomplete on Standard Addresses

When you enable autocomplete on standard addresses, Salesforce app users can enter text on standard address fields and see possible matching addresses in a picklist.

Autocomplete on standard address picklist results are optimized for these countries:

- USA
- Japan
- United Kingdom
- Canada
- Australia
- Germany
- France
- Netherlands
- Brazil
- Spain

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Professional**, **Enterprise**, **Performance**, and **Unlimited** editions.

USER PERMISSIONS

To modify maps and location settings:

- Customize Application

- Russia
- Sweden

To enable autocomplete on standard address fields:

1. From Setup, enter `Maps` in the `Quick Find` box, select **Maps and Location Settings**, then click **Edit**.
2. Check `Enable autocomplete on standard address fields`.
3. Click **Save**.

Note:

- Autocomplete on standard address fields is available for all versions of the Salesforce app and Lightning Experience.

Let Users Select State and Country from Picklists

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions except Database.com

State and country picklists let users select states and countries from predefined, standardized lists, instead of entering state and country data into text fields. State and country picklists offer faster and easier data entry. They help to ensure cleaner data that can be harnessed for other uses—in reports and dashboards, for example. They protect data integrity by preventing typos, alternate spellings, and junk data—even in records updated through the API.

The states and countries in the picklists are based on ISO-3166 standard values, making them compatible with other applications.

State and country picklists are available in the shipping, billing, mailing, and "other" address fields in the account, campaign members, contact, contract, lead, order, person accounts, quotes, and service contracts standard objects. The picklists are also available for managing users and companies in Setup. To use the picklists, first choose the country and then choose from the options that automatically populate the state or province picklist.

You can use the state and country picklists in most places that state and country fields are available in Salesforce, including:

- Record edit and detail pages
- List views, reports, and dashboards
- Filters, functions, rules, and assignments

State and country picklists can also be searched, and they're supported in Translation Workbench.

State and Country Picklist Limitations

State and country picklists include 239 countries by default. They also include the states and provinces of the United States, Canada, Australia, Brazil, China, India, Ireland, Italy, and Mexico. State and country picklists that contain more than 1,000 states or countries can cause degraded performance. State and country picklists do not work with:

- Salesforce to Salesforce
- Salesforce Mobile Classic
- Connect Offline
- Visual Workflow or change sets

If your org uses Data.com, the Data.com records can contain states and countries not included in the standard state and country picklists. If your org uses these states and countries, add them to the picklist before Data.com users can add or clean these records:

- American Samoa (AS)
- Guam (GU)
- Hong Kong (HK)

- Marshall Islands (MH)
- Netherlands Antilles (AN)
- Northern Mariana Islands (MP)
- Serbia and Montenegro (CS)
- United States Minor Outlying Islands (UM)

Picklist labels, not code values, are displayed in reports on state and country fields. To display code value abbreviations wherever your users see state or country names, manually change your State Name or Country Name labels to your code values. (For editing instructions, see Configure State and Country Picklists on page 149.) You can access your records' state and country code values by using the `StateCode` and `CountryCode` fields in Workbench or the Data Loader.

Implementing State and Country Picklists

Here's how to transition from text-based state and country fields to state and country picklists.

1. Configure the state and country values you want to use in your org.

   We recomment this step because it gives you the opportunity to customize state and country values. It ensures that state and country data continues to work with the third-party systems you have integrated with Salesforce.

2. Scan your org's data and customizations.

   Convert data and update customizations, such as list views, reports, and workflow rules, so that they continue to work with the new field type.

3. Convert existing data.

   The conversion process lets you map the various values in your org to standard picklist values. For example, map U.S., USA, and United States to US.

4. Turn on the picklists for your users.

   If you turn on state and country picklists without configuring values, scanning your org, and converting existing data, users can use the picklists in new records. However, all existing data is incompatible with the new format, which could compromise data consistency and integrity across the two field formats.

5. Optionally, rescan and fix customizations or records that have been created or edited since your first scan.

For a step-by-step guide to implementing state and country picklists, see Implementing State and Country Picklists.

IN THIS SECTION:

Integration Values for State and Country Picklists

An integration value is a customizable text value that is linked to a state or country code. Integration values for standard states and countries default to the full ISO-standard state and country names. Integration values function similarly to the API names of custom fields and objects. Configuring integration values allows integrations that you set up before enabling state and country picklists to continue to work.

Configure State and Country Picklists

Configuring state and country picklists means choosing which states and countries you want to be available in your Salesforce org. It lets you make state and country picklists available for purposes like importing data, working with external systems, and accessing picklist data from the Metadata API.

Standard Countries for Address Picklists

Edit State and Country Details

You can add states and countries to your organization or edit the values of existing states and countries on a state or country's detail page.

State and Country Picklists and the Metadata API

If you're editing many state and country picklist integration values, using the Metadata API is more efficient than editing values in Setup.

Prepare to Scan State and Country Data and Customizations

Before switching from text-based state and country fields to standardized state and country picklists, scan your org to see how the change affects it. This discovery process shows you where and how state and country data appears in your org. The process also shows where this data is used in customizations, such as list views and reports. After you've analyzed the scan results, you can plan to convert your data, update your customizations, and turn on state and country picklists.

Scan State and Country Data and Customizations

Prepare to Convert State and Country Data

If your Salesforce organization includes text-based state and country values, you can convert that data to standardized picklist values.

Convert State and Country Data

To convert text-based state and country data to picklist-compatible values, select specific text values and choose the standard values you want to map them to. For example, you can select all occurrences of "USA" and change them to "United States."

Enable and Disable State and Country Picklists

When you enable state and country picklists, the picklists are immediately available to users. However, it can take some time for Salesforce to populate the ISO code fields on existing records. If users try to edit the state or country on a record before the code field is populated, they are prompted to select a code value.

State and Country Picklist Field-Syncing Logic

When you save records with state and country picklist values, Salesforce syncs the records' integration and code values for states and countries. You can't directly edit state or country integration values on record detail pages. You can directly edit records' state or country integration values only with workflows, Apex code, API integrations, and so on.

State and Country Picklist Error Messages

When you try to save records with mismatched code and text values for states or countries, various errors can occur. This information demystifies those error messages.

Integration Values for State and Country Picklists

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions except Database.com

An integration value is a customizable text value that is linked to a state or country code. Integration values for standard states and countries default to the full ISO-standard state and country names. Integration values function similarly to the API names of custom fields and objects. Configuring integration values allows integrations that you set up before enabling state and country picklists to continue to work.

When you enable state and country picklists, your text-typed `State/Province` and `Country` fields are repurposed as `Integration Value` fields. In reports and list views, your `Integration Value` fields are called `State/Province (text only)` and `Country (text only)`. In addition, for each of your `State/Province (text only)` and `Country (text only)` fields, a picklist-typed `State Code` or `Country Code` field is created. The state and country picklist values set up in your organization determine the available values on these code fields.

Among the fields on each state or country picklist value are `Active`, `Visible`, `Name`, `Code`, and `Integration Value`. All your state and country picklists—for `Billing Address`, `Shipping Address`, and so on—can access the state and country picklist values you create. Storing a state or country code allows your records to access other information about your states and countries.

By default, `Name` and `Integration Value` fields for your states and countries contain identical values. The value in the `Name` field displays to users who interact with your picklist. `Integration Value` is used by:

- Apex classes and triggers
- Visualforce pages
- SOQL queries
- API queries and integrations
- Rules for assignment, AutoResponse, validation, and escalation
- Workflow rules
- Email templates
- Custom buttons and links
- Field set customizations
- Reports and list views

When you update a code value on a record, that record's `State/Province (text only)` or `Country (text only)` column is populated with the corresponding integration value. Likewise, when you update a state or country `(text only)` column with a valid integration value, we keep the corresponding state or country code column in sync. You can change your organization's integration values after you enable state and country picklists. However, when you update your picklists' state and country integration values, the integration values on your records aren't updated. Name values aren't stored on records. Instead, they're retrieved from Salesforce based on a record's `State Code` or `Country Code` value. If the states or countries in your picklists have different field values for `Name` and `Integration Value`, make sure your report or list view filters use the correct values. Use names in `State` and `Country` filters, and use integration values in `State (text only)` and `Country (text only)` filters. Otherwise, your reports can fail to capture all relevant records.

Edit your integration values in Setup or using the Metadata API. States' and countries' `Name` fields are editable only in Setup. In the Metadata API, `Name` and `Integration Value` fields are called `label` and `integrationValue`, respectively.

SEE ALSO:

Let Users Select State and Country from Picklists

Edit State and Country Details

State and Country Picklist Field-Syncing Logic

State and Country Picklist Error Messages

Configure State and Country Picklists

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions except Database.com

USER PERMISSIONS

To configure state and country picklists:
- Modify All Data

Configuring state and country picklists means choosing which states and countries you want to be available in your Salesforce org. It lets you make state and country picklists available for purposes like importing data, working with external systems, and accessing picklist data from the Metadata API.

Configuring picklists is not required for you to enable state and country picklists for users, but it's highly recommended. Configuring picklists helps ensure continuity and data integrity with existing state and country data and customizations.

When configuring states and countries, you start with countries and drill down to their states or provinces. State and country picklists include 239 countries by default. They also include the states and provinces of the United States, Canada, Australia, Brazil, China, India, Ireland, Italy, and Mexico. State and country picklists that contain more than 1,000 states or countries can cause degraded performance. For the complete list of default countries, see Standard Countries for Address Picklists.

Note:

- Integration values for state and country picklists can also be configured through the Metadata API. For more information, read about the AddressSettings component in the *Metadata API Developer Guide*.
- State and country picklists aren't supported in Salesforce change sets or packages. However, you can move integration value changes for state and country picklists between sandbox and production orgs by using the Metadata API. First, configure your state and country picklists in your sandbox org. Then, use the Metadata API to retrieve the sandbox configurations, and deploy them to your production org. You can't deploy new ISO codes or update ISO code values using any API.

1. From Setup, enter `State and Country Picklists` in the `Quick Find` box, then select **State and Country Picklists**.
2. On the State and Country Picklists setup page, click **Configure states and countries**.
3. Select from the following options:

   `Active`
   Makes the country available in the Metadata API so that records that contain the country can be imported. However, unless you also set it as visible, the country isn't available to users in Salesforce.

   `Visible`
   Makes the country available to users in Salesforce. A country has to be active before you can make it visible.

4. Click **Edit** to view and edit details for the country, including to configure its states or provinces.
5. (Optional) Under Picklist Settings, select a `Default Country`. The Default Country automatically populates country picklists for new records in your org, but users can select a different country. Default countries must be both active and visible.
6. Click **Save** to save your configuration.

Note: Active states and countries not marked `Visible` are still valid filter lookup values. You can use invisible states and countries when creating filters in reports, list views, workflows, and so on.

SEE ALSO:

Edit State and Country Details

Let Users Select State and Country from Picklists

Integration Values for State and Country Picklists

Standard Countries for Address Picklists

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions except Database.com

Standard Countries

Salesforce provides these 239 countries as standard for country address picklists. An asterisk (*) indicates that states or provinces are available for that country.

ISO Code	Country
AD	Andorra
AE	United Arab Emirates
AF	Afghanistan
AG	Antigua and Barbuda
AI	Anguilla
AL	Albania
AM	Armenia
AO	Angola
AQ	Antarctica
AR	Argentina
AT	Austria
AU	Australia*
AW	Aruba
AX	Aland Islands
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BD	Bangladesh
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BH	Bahrain
BI	Burundi
BJ	Benin
BL	Saint Barthélemy
BM	Bermuda

ISO Code	Country
BN	Brunei Darussalam
BO	Bolivia, Plurinational State of
BQ	Bonaire, Sint Eustatius and Saba
BR	Brazil*
BS	Bahamas
BT	Bhutan
BV	Bouvet Island
BW	Botswana
BY	Belarus
BZ	Belize
CA	Canada*
CC	Cocos (Keeling) Islands
CD	Congo, the Democratic Republic of the
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Cote d'Ivoire
CK	Cook Islands
CL	Chile
CM	Cameroon
CN	China*
CO	Colombia
CR	Costa Rica
CU	Cuba
CV	Cape Verde
CW	Curaçao
CX	Christmas Island
CY	Cyprus
CZ	Czech Republic
DE	Germany

ISO Code	Country
DJ	Djibouti
DK	Denmark
DM	Dominica
DO	Dominican Republic
DZ	Algeria
EC	Ecuador
EE	Estonia
EG	Egypt
EH	Western Sahara
ER	Eritrea
ES	Spain
ET	Ethiopia
FI	Finland
FJ	Fiji
FK	Falkland Islands (Malvinas)
FO	Faroe Islands
FR	France
GA	Gabon
GB	United Kingdom
GD	Grenada
GE	Georgia
GF	French Guiana
GG	Guernsey
GH	Ghana
GI	Gibraltar
GL	Greenland
GM	Gambia
GN	Guinea
GP	Guadeloupe
GQ	Equatorial Guinea

ISO Code	Country
GR	Greece
GS	South Georgia and the South Sandwich Islands
GT	Guatemala
GW	Guinea-Bissau
GY	Guyana
HM	Heard Island and McDonald Islands
HN	Honduras
HR	Croatia
HT	Haiti
HU	Hungary
ID	Indonesia
IE	Ireland*
IL	Israel
IM	Isle of Man
IN	India*
IO	British Indian Ocean Territory
IQ	Iraq
IR	Iran, Islamic Republic of
IS	Iceland
IT	Italy*
JE	Jersey
JM	Jamaica
JO	Jordan
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KH	Cambodia
KI	Kiribati
KM	Comoros
KN	Saint Kitts and Nevis

ISO Code	Country
KP	Korea, Democratic People’s Republic of
KR	Korea, Republic of
KW	Kuwait
KY	Cayman Islands
KZ	Kazakhstan
LA	Lao People’s Democratic Republic
LB	Lebanon
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
LY	Libyan Arab Jamahiriya
MA	Morocco
MC	Monaco
MD	Moldova, Republic of
ME	Montenegro
MF	Saint Martin (French part)
MG	Madagascar
MK	Macedonia, the former Yugoslav Republic of
ML	Mali
MM	Myanmar
MN	Mongolia
MO	Macao
MQ	Martinique
MR	Mauritania
MS	Montserrat

ISO Code	Country
MT	Malta
MU	Mauritius
MV	Maldives
MW	Malawi
MX	Mexico*
MY	Malaysia
MZ	Mozambique
NA	Namibia
NC	New Caledonia
NE	Niger
NF	Norfolk Island
NG	Nigeria
NI	Nicaragua
NL	Netherlands
NO	Norway
NP	Nepal
NR	Nauru
NU	Niue
NZ	New Zealand
OM	Oman
PA	Panama
PE	Peru
PF	French Polynesia
PG	Papua New Guinea
PH	Philippines
PK	Pakistan
PL	Poland
PM	Saint Pierre and Miquelon
PN	Pitcairn
PS	Palestine

ISO Code	Country
PT	Portugal
PY	Paraguay
QA	Qatar
RE	Reunion
RO	Romania
RS	Serbia
RU	Russian Federation
RW	Rwanda
SA	Saudi Arabia
SB	Solomon Islands
SC	Seychelles
SD	Sudan
SE	Sweden
SG	Singapore
SH	Saint Helena, Ascension and Tristan da Cunha
SI	Slovenia
SJ	Svalbard and Jan Mayen
SK	Slovakia
SL	Sierra Leone
SM	San Marino
SN	Senegal
SO	Somalia
SR	Suriname
SS	South Sudan
ST	Sao Tome and Principe
SV	El Salvador
SX	Sint Maarten (Dutch part)
SY	Syrian Arab Republic
SZ	Swaziland
TC	Turks and Caicos Islands

ISO Code	Country
TD	Chad
TF	French Southern Territories
TG	Togo
TH	Thailand
TJ	Tajikistan
TK	Tokelau
TL	Timor-Leste
TM	Turkmenistan
TN	Tunisia
TO	Tonga
TR	Turkey
TT	Trinidad and Tobago
TV	Tuvalu
TW	Taiwan
TZ	Tanzania, United Republic of
UA	Ukraine
UG	Uganda
US	United States*
UY	Uruguay
UZ	Uzbekistan
VA	Holy See (Vatican City State)
VC	Saint Vincent and the Grenadines
VE	Venezuela, Bolivarian Republic of
VG	Virgin Islands, British
VN	Vietnam
VU	Vanuatu
WF	Wallis and Futuna
WS	Samoa
YE	Yemen
YT	Mayotte

ISO Code	Country
ZA	South Africa
ZM	Zambia
ZW	Zimbabwe

Edit State and Country Details

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions except Database.com

USER PERMISSIONS

To add or edit state or country details:

- Modify All Data

You can add states and countries to your organization or edit the values of existing states and countries on a state or country's detail page.

To add or edit a state or province, navigate to its detail page through the detail page of its associated country.

1. From Setup, enter *`State`* in the `Quick Find` box, then select **State and Country Picklists**.
2. Click **Configure states and countries**.
3. Click **New Country** to add a country or click **Edit** for a listed country.
4. Under Country Information, specify your options.

   `Country Name`

   By default, the ISO-standard name. The name is what users see in the Salesforce user interface.

   `Country Code`

   By default, the two-letter ISO-standard code. If you change an ISO code, the new value must be unique. Codes are case insensitive and must contain only ASCII characters and numbers. You can't edit the ISO codes of standard states or countries. You can edit the country codes of custom states and countries only before you enable those states and countries for your users.

   `Integration Value`

   A customizable text value that is linked to a state or country code. Integration values for standard states and countries default to the full ISO-standard state and country names. Integration values function similarly to the API names of custom fields and objects. Configuring integration values allows integrations that you set up before enabling state and country picklists to continue to work.

   You can edit integration values to match values that you use elsewhere in your organization. For example, let's say that you have a workflow rule that uses `USA` instead of the default `United States` as the country name. If you manually set the integration value for country code `US` to *`USA`*, the workflow rule doesn't break when you enable state and country picklists.

   When you update a code value on a record, that record's `State/Province (text only)` or `Country (text only)` column is populated with the corresponding integration value. Likewise, when you update a state or country `(text only)` column with a valid integration value, we keep the corresponding state or country code column in sync. You can change your organization's integration values after you enable state and country picklists. However, when you update your picklists' state and country integration values, the integration values on your records aren't updated. Name values aren't stored on records. Instead, they're retrieved from Salesforce based on a record's `State Code` or `Country Code` value. If the states or countries in your picklists have different field values for `Name` and `Integration Value`, make sure your report or list view filters use the correct values. Use names in `State` and `Country` filters, and use integration values in `State (text only)` and `Country (text only)` filters. Otherwise, your reports can fail to capture all relevant records.

`Active`
Makes the country available in the Metadata API so that records can be imported that contain the country. However, unless you also set it as visible, the country isn't available to users in Salesforce.

`Visible`
Makes the country available to users in Salesforce. A country must be active before you can make it visible.

5. If you're adding a country, click **Add**.
6. If you're editing a country, specify the options for States:

   `Active`
   Makes the state available in the Metadata API so that records can be imported that contain the state. However, unless you also set it as visible, the state isn't available to users in Salesforce.

   `Visible`
   Makes the state available to users in Salesforce. A state must be active before you can make it visible.

7. Click either of the following, if desired.
   - **New State** to add a custom state or province. On the New State page, specify a `State Name`, `State Code`, and `Integration Value`, and select whether the new state is `Active` or `Visible`. To save the new state, click **Add**.
   - **Edit** to view and edit state or province details, including the `State Name`, `State Code`, and `Integration Value`.
8. Click **Save**.

SEE ALSO:

Configure State and Country Picklists

Let Users Select State and Country from Picklists

Integration Values for State and Country Picklists

State and Country Picklists and the Metadata API

State and Country Picklists and the Metadata API

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions except Database.com

If you're editing many state and country picklist integration values, using the Metadata API is more efficient than editing values in Setup.

You can use the Metadata API to edit existing states and countries in state and country picklists. You can't use the Metadata API to create or delete new states or countries. First, configure your state and country picklists in your sandbox org. Then, use the Metadata API to retrieve the sandbox configurations, and deploy them to your production org. You can't deploy new ISO codes or update ISO code values using any API. Search for "AddressSettings" in the *Metadata API Developer Guide* for information about working with state and country picklists in the Metadata API.

SEE ALSO:

Integration Values for State and Country Picklists

Edit State and Country Details

Prepare to Scan State and Country Data and Customizations

Before switching from text-based state and country fields to standardized state and country picklists, scan your org to see how the change affects it. This discovery process shows you where and how state and country data appears in your org. The process also shows where this data is used in customizations, such as list views and reports. After you've analyzed the scan results, you can plan to convert your data, update your customizations, and turn on state and country picklists.

Every org's discovery process is unique. For some orgs, transitioning from state and country text fields to standardized picklists is straightforward and manageable. However, if state and country metadata is used extensively throughout an org, the transition can be a complicated and time-consuming process. Salesforce recommends that you scan your org early and often so that you can transition smoothly to the new lists. Keep these best practices and considerations in mind.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions except Database.com

- Scanning doesn't convert data or fix your customizations. Convert your data separately, and update your customizations individually.
- You can continue to work normally in your org during the scan.
- The scanning process identifies affected managed packages but doesn't provide a mechanism for addressing packaging issues.
- Scanning doesn't find formulas that include state and country metadata.
- You can't use display values in validation rules or workflow rules that use comparison formula functions. If your validation or workflow rules on state or country fields use `BEGINS`, `CONTAINS`, `ISCHANGED`, or `REGEX`, use `ISPICKVAL` with state and country code values in your comparison functions.
- Scanning doesn't find personal list views and reports that use state and country metadata. Individual users must update those customizations themselves.
- Converted leads aren't scanned. State and country values aren't updated on converted lead records when you enable state and country picklists.
- Scan your org multiple times. After you update a customization, rescan to make sure that your changes fixed the problem and didn't create new ones.

SEE ALSO:

Scan State and Country Data and Customizations

Let Users Select State and Country from Picklists

Scan State and Country Data and Customizations

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions except Database.com

USER PERMISSIONS

To scan state and country data and customizations:

- Modify All Data

  AND

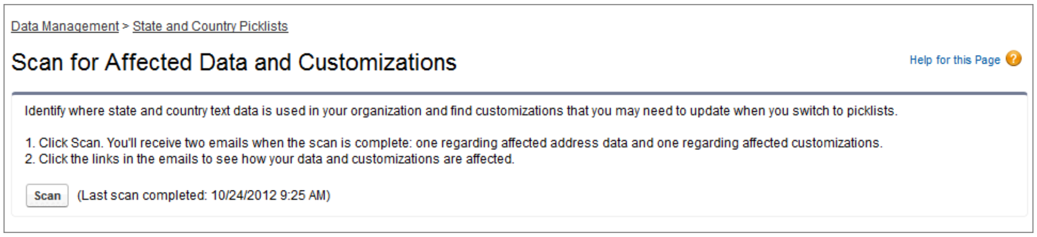
  Create Documents

Scanning an organization for text-based state and country values reveals where and how text-based state and country data appears in existing records. For example, you can see all the ways United States is saved as a text value, such as U.S., US, America, Estados Unidos, and even misspelled entries like Untied States. In addition, scanning shows you where state and country data is used in customizations, including:

- List views
- Reports
- Validation rules
- Custom buttons and links
- Workflow rules
- Email templates
- Field sets
- Apex classes and triggers
- Visualforce pages

When the scan is complete, you receive 2 emails with links to detailed reports: one on address data and one on customizations. After analyzing the reports, begin the tasks of converting existing data to picklist values and updating customizations so that they work with the new picklist fields.

1. From Setup, enter `State and Country Picklists` in the `Quick Find` box, then select **State and Country Picklists**.
2. On the State and Country Picklists setup page, click **Scan Now** and then click **Scan**.



Data Management > State and Country Picklists

Scan for Affected Data and Customizations

Identify where state and country text data is used in your organization and find customizations that you may need to update when you switch to picklists.

1. Click Scan. You'll receive two emails when the scan is complete: one regarding affected address data and one regarding affected customizations.
2. Click the links in the emails to see how your data and customizations are affected.

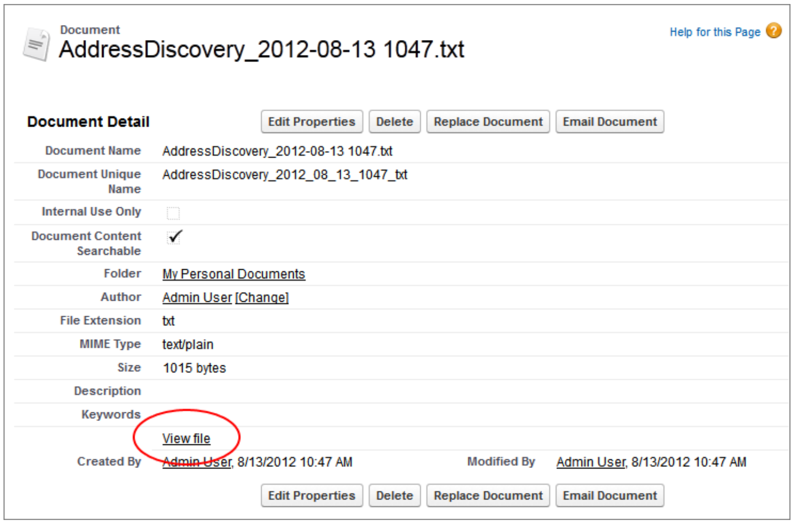
(Last scan completed: 10/24/2012 9:25 AM)

3. Wait for an email that contains the results.

   Depending on the size and complexity of your organization, the results take anywhere between a few minutes and a few hours to generate.

   Note: The emails are sent from noreply@salesforce.com. They have the subject line, “Salesforce Address Data Scan” or “Salesforce Address Customization Scan.” If you don’t receive the emails, make sure that they weren’t caught in a spam filter.

4. Click the link in each email to go to a document that contains the report of affected data or customizations.
5. On the Document detail page, click **View file**.



Document

AddressDiscovery_2012-08-13 1047.txt

Help for this Page

Document Detail Edit Properties | Delete | Replace Document | Email Document

Document Name	AddressDiscovery_2012-08-13 1047.txt
Document Unique Name	AddressDiscovery_2012_08_13_1047_txt
Internal Use Only	□
Document Content Searchable	✓
Folder	My Personal Documents
Author	Admin User [Change]
File Extension	txt
MIME Type	text/plain
Size	1015 bytes
Description	
Keywords	
	View file
Created By	Admin User, 8/13/2012 10:47 AM
Modified By	Admin User, 8/13/2012 10:47 AM

Edit Properties | Delete | Replace Document | Email Document

SEE ALSO:

Let Users Select State and Country from Picklists

Prepare to Convert State and Country Data

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions except Database.com

If your Salesforce organization includes text-based state and country values, you can convert that data to standardized picklist values.

Converting existing data allows you to keep working with the data after you switch to picklists. Say, you have a report that culls all your sales reps' leads in Washington state. The report is generated from state picklist value Washington. To ensure that records with text-based state values such as Wash., WA, and Washington are included in the report, convert text-based state data to standardized picklist values.

Converting existing state and country text data into standardized picklist values helps ensure data integrity after you enable picklists in your organization. Your users encounter validation errors when saving records that contain state or country values not in your picklists. Also, reports become unreliable when records created before you enable state and country picklists contain different state and country values than records created using picklists.

When you convert data, Salesforce starts with countries, then goes on to states. As you go through the conversion process, here are a few things to keep in mind:

- Save frequently. You can exit the conversion tool and return to it at any time.
- You can continue to work normally in your organization while converting data.
- You can't convert data while you're scanning for affected data and customizations, or while state or country picklists are being deployed.
- Steps can be repeated and undone at any time until you enable the picklists for users. After the picklists are enabled, you can't undo the conversion.

- If you use Data.com Clean, we recommend that you suspend Clean jobs until the conversion is finished.

SEE ALSO:

Convert State and Country Data

Let Users Select State and Country from Picklists

Convert State and Country Data

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions except Database.com

USER PERMISSIONS

To convert text-based state and country data:

- Modify All Data

To convert text-based state and country data to picklist-compatible values, select specific text values and choose the standard values you want to map them to. For example, you can select all occurrences of "USA" and change them to "United States."

Before you convert state and country values in State and Country Picklists setup, configure the picklists for your org. That way, the data in your org is consistent and accurate when you enable picklists, because all new and updated records use your specified integration value.

Convert countries first, and then states and provinces.

You can convert up to 2,000 country values and up to 2,000 state values. However, state and country picklists that contain more than 1,000 states or countries can degrade performance.

1. From Setup, enter *`State and Country Picklists`* in the `Quick Find` box, then select **State and Country Picklists**.
2. On the State and Country Picklists setup page, click **Convert now**.
   Salesforce opens the Convert Countries page. This page displays all the country text values that appear in your org and the number of times each value is used.
3. Select `Change` for one or more values you want to convert. For example, select `Change` for all the iterations of United States.
4. In the `Change To` area, choose the country you want to convert the text values to and click **Save to Changelist**.

   Note: If you map states or countries to `Unknown value`, users see states and countries in their records. However, your users encounter errors when they save records, unless they change each state or country to a valid value before saving.

5. Repeat Steps 3 and 4 for other country values, such as for Canada.
   Salesforce tracks planned changes in the Changelist area.
6. When all the countries are mapped, click **Next** to convert state values.

   Use the Country of Origin column to identify the country associated with that state or province.

7. On the Confirm Changes page, click **Finish** to return to the setup overview page. Or click **Finish and Enable Picklists** to convert the values and turn on state and country picklists in your org.

A few words about undo:

- On the Convert Countries or Convert States page, click **Undo** at any time to revert values in the changelist.
- On the Convert States page, click **Previous** to return to the Convert Countries page and change country mappings.
- You can convert state and country values even after clicking **Finish**. After picklists are enabled, however, you can no longer edit your conversion mappings.

SEE ALSO:

Let Users Select State and Country from Picklists

Enable and Disable State and Country Picklists

When you enable state and country picklists, the picklists are immediately available to users. However, it can take some time for Salesforce to populate the ISO code fields on existing records. If users try to edit the state or country on a record before the code field is populated, they are prompted to select a code value.

1. From Setup, enter `State and Country Picklists` in the `Quick Find` box, then select **State and Country Picklists**.
2. On the State and Country Picklists setup page, click **Enable** to turn on the picklists.

   Note:

   - You can also enable state and country picklists when you finish converting existing, text-based data to picklist values. See Convert State and Country Data.

3. To turn off state and country picklists, click **Disable** on the State and Country Picklists setup page.

   Important: If you disable state and country picklists:

   - For records that you haven't saved since enabling picklists, state and country values revert to their original text values.
   - For records that you have saved since enabling picklists, state and country integration values replace original text values.
   - References to state and country picklists in customizations—such as workflow field updates, email templates, and Visualforce pages—become invalid.
   - Columns and filters that refer to picklist fields in reports and list views disappear.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions except Database.com

USER PERMISSIONS

To turn state and country picklists on and off:

- Modify All Data

SEE ALSO:

Let Users Select State and Country from Picklists

State and Country Picklist Field-Syncing Logic

When you save records with state and country picklist values, Salesforce syncs the records' integration and code values for states and countries. You can't directly edit state or country integration values on record detail pages. You can directly edit records' state or country integration values only with workflows, Apex code, API integrations, and so on.

Your Change	Result
You update a record's state or country code to a valid value.	Salesforce updates the record's state or country integration value to match the code.
You update a record's state or country integration value to a valid value.	Salesforce updates the record's state or country code to match the integration value.
You remove a record's country code, but don't remove the corresponding state code.	Salesforce removes the record's state code and the state and country integration values.
You create or update a record with state and country values. The new state isn't in the new country.	No changes are saved. You get an error message.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions except Database.com

Your Change	Result
You update the state or country integration and code values on an existing record. The new integration and code values don't match.	No changes are saved. You get an error message.
You create a record with mismatched state or country integration and code values.	Salesforce updates your new record's integration value to match the code value.

SEE ALSO:

- Let Users Select State and Country from Picklists
- Integration Values for State and Country Picklists
- State and Country Picklist Error Messages

State and Country Picklist Error Messages

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions except Database.com

When you try to save records with mismatched code and text values for states or countries, various errors can occur. This information demystifies those error messages.

Error	Cause
Invalid country specified for field	Your country code doesn't match an existing country.
There's a problem with this country, even though it may appear correct. Please select a country from the list of valid countries.	Your country integration value doesn't match an existing country. Or, the country value was mapped to `Unknown value` during data conversion.
Mismatched integration value and ISO code for field	Your code and integration values match different states or countries.
A country must be specified before specifying a state value for field	Your record has a state code or integration value but no country code. You can't save a state without a corresponding country.
The existing country doesn't recognize the state value for field	Your state code and integration values belong to a state in a different country.
Invalid state specified for field	Your state code doesn't match an existing state.

SEE ALSO:

- Let Users Select State and Country from Picklists
- Integration Values for State and Country Picklists
- State and Country Picklist Field-Syncing Logic

Customize Reports and Dashboards

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

To get to this page, from Setup, enter `Reports` in the `Quick Find` box, then select **Reports and Dashboards Settings**.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

IN THIS SECTION:

Enable the Lightning Report Builder (Beta)

Turn on the Lightning report builder and give your users a powerful, intuitive tool for analyzing Salesforce data. Users can group, filter, and summarize records to answer business questions like "Which lead source generates the most closed opportunities?"

Enable Lightning Tables, the Dashboard Component (Beta)

The Lightning table, a new dashboard table component, shows up to 10 columns from source reports. The columns available to be added to a Lightning table are added from the source report's report type's available fields. The fields need not be added as a column on the source report. Add a Lightning table to your dashboard to supplement chart and metric based overviews with record-by-record details.

Provide Convenience Features for Your Report and Dashboard Users

You can enable or disable several user interface features that may help your users get more out of reports and dashboards. These settings are for convenience and ease of use; they don't affect the data returned in your reports and dashboards.

Let Users Subscribe to Report Notifications

Allow users to subscribe to reports to be notified whenever certain metrics meet conditions they specify.

Customize Report and Dashboard Email Notifications

Choose how users are notified when information changes in the reports and dashboards they use.

Set Up a Custom Report Type

A *report type* defines the set of records and fields available to a report based on the relationships between a primary object and its related objects. Reports display only records that meet the criteria defined in the report type.

Turn On Enhanced Folder Sharing for Reports and Dashboards

When you enable folder sharing, Salesforce converts your users' existing folder access levels to use new, more detailed access levels.

Set Up Historical Trend Reporting

To make historical trend reports available to your users, start by using filters to configure the amount of data that's captured for historical trend reporting. Then select the fields needed for historical reports.

Upgrade the Report Wizard

Report builder, a powerful drag-and-drop editor, is the standard tool for creating and editing reports. If your organization is still using the old report wizard, you should upgrade to report builder.

SEE ALSO:

Upgrade the Report Wizard

Enable the Lightning Report Builder (Beta)

Turn on the Lightning report builder and give your users a powerful, intuitive tool for analyzing Salesforce data. Users can group, filter, and summarize records to answer business questions like "Which lead source generates the most closed opportunities?"

Available in: Lightning Experience

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

Available in: Enhanced Folder Sharing

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

After enabling the Lightning Experience report builder, users can still access the Salesforce Classic report builder.

1. From Setup, enter *`Reports`* in the `Quick Find` box, then select **Reports and Dashboards Settings**.
2. Select **Enable Lightning Report Builder (Beta)**.
3. Click **Save**.
4. To grant access to the Lightning report builder, assign people the user permission "Report Builder (Lightning Experience)".

The Lightning Report builder becomes available from the Reports tab.

Enable Lightning Tables, the Dashboard Component (Beta)

The Lightning table, a new dashboard table component, shows up to 10 columns from source reports. The columns available to be added to a Lightning table are added from the source report's report type's available fields. The fields need not be added as a column on the source report. Add a Lightning table to your dashboard to supplement chart and metric based overviews with record-by-record details.

1. From Setup, enter *`Dashboards`* in the `Quick Find` box, then select **Reports and Dashboards Settings**.
2. Select **Enable Lightning Dashboard Tables (Beta)**.
3. Click **Save**.

Lightning dashboard table components become available in the Lightning Experience dashboard builder.

EDITIONS

Available in: Lightning Experience

Available in: **Group** (View Only), **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Available in: both Legacy Folder Sharing and Enhanced Folder Sharing

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

Provide Convenience Features for Your Report and Dashboard Users

You can enable or disable several user interface features that may help your users get more out of reports and dashboards. These settings are for convenience and ease of use; they don't affect the data returned in your reports and dashboards.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

IN THIS SECTION:

Let Users See Report Headers While Scrolling

Floating report headers keep column and row headings in sight no matter how far users scroll in report results.

Help Users Find Dashboards Quickly

Dashboard finder uses auto-complete to help users quickly find dashboards in the Dashboards tab, just by entering the first few letters of its name in the search filter.

Let Users Post Dashboard Components in Chatter

Dashboard component snapshots let users post static images of dashboard components to Chatter feeds, making the snapshot visible to all users.

Exclude the Confidential Information Disclaimer from Reports

By default, report footers include a disclaimer that reads "Confidential Information - Do Not Distribute". The disclaimer reminds users to be mindful of who they share reports with, helping to ensure that third parties don't view your reports. At your discretion, exclude the disclaimer from your reports.

Show Enhanced Charts in the Salesforce App

Show your users enhanced charts in the Salesforce app. Enhanced charts are similar to Lightning Experience charts: see details before drilling into a report, filter reports by tapping on chart segments, and change chart types. This feature is available in all versions of the Salesforce app.

Let Users See Report Headers While Scrolling

Floating report headers keep column and row headings in sight no matter how far users scroll in report results.

With floating report headers, users can scroll to the bottom of lengthy reports without having to scroll back to the top to view the names of the column headings.

Users can also click floating report headers to sort data in a specific column. When users sort data by clicking a floating report heading, the report refreshes and redirects users to the beginning of report results.

Floating headers are available for tabular, summary, and matrix reports.

1. From Setup, enter `Reports` in the `Quick Find` box, then select **Reports and Dashboards Settings**.
2. Select or deselect **Enable Floating Report Headers**.
3. Click **Save**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Group** (View Only), **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

Help Users Find Dashboards Quickly

Dashboard finder uses auto-complete to help users quickly find dashboards in the Dashboards tab, just by entering the first few letters of its name in the search filter.

All dashboards matching that text are dynamically displayed in the drop-down list. The list first shows dashboards the user viewed recently, and then other dashboards appear in alphabetical order by folder. The first 1000 results are shown in a single list; above 1000, results are shown 500 per page. Users only see dashboards in folders they can access. Disable this option to use the static drop-down list instead.

This option is enabled by default.

1. From Setup, enter `Reports` in the `Quick Find` box, then select **Reports and Dashboards Settings**.
2. Select or deselect **Enable Dashboard Finder**.
3. Click **Save**.

EDITIONS

Available in: Salesforce Classic

Available in: **Group** (View Only), **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Available in: both Legacy Folder Sharing and Enhanced Folder Sharing

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

Let Users Post Dashboard Components in Chatter

Dashboard component snapshots let users post static images of dashboard components to Chatter feeds, making the snapshot visible to all users.

1. Make sure Chatter feed tracking for dashboards is enabled.
2. From Setup, enter `Reports` in the `Quick Find` box, then select **Reports and Dashboards Settings**.
3. Select or deselect **Enable Dashboard Component Snapshots**.

Important: This option lets users override dashboard visibility settings, making snapshots visible to all Chatter users. Though this makes it easy to share time-specific data without having to add people to dashboard folders, be aware that users can inadvertently post sensitive or confidential information.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Group** (View Only), **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Available in: both Legacy Folder Sharing and Enhanced Folder Sharing

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

Exclude the Confidential Information Disclaimer from Reports

By default, report footers include a disclaimer that reads "Confidential Information - Do Not Distribute". The disclaimer reminds users to be mindful of who they share reports with, helping to ensure that third parties don't view your reports. At your discretion, exclude the disclaimer from your reports.

1. From Setup, enter *`Reports and Dashboards Settings`* in the `Quick Find` box, then select **Reports and Dashboards Settings**.
2. Select **Exclude Disclaimer from Exported Reports** and **Exclude Disclaimer from Report Run Pages and from Printable View Pages**.
3. Click **Save**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Group** (View Only), **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

Show Enhanced Charts in the Salesforce App

Show your users enhanced charts in the Salesforce app. Enhanced charts are similar to Lightning Experience charts: see details before drilling into a report, filter reports by tapping on chart segments, and change chart types. This feature is available in all versions of the Salesforce app.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

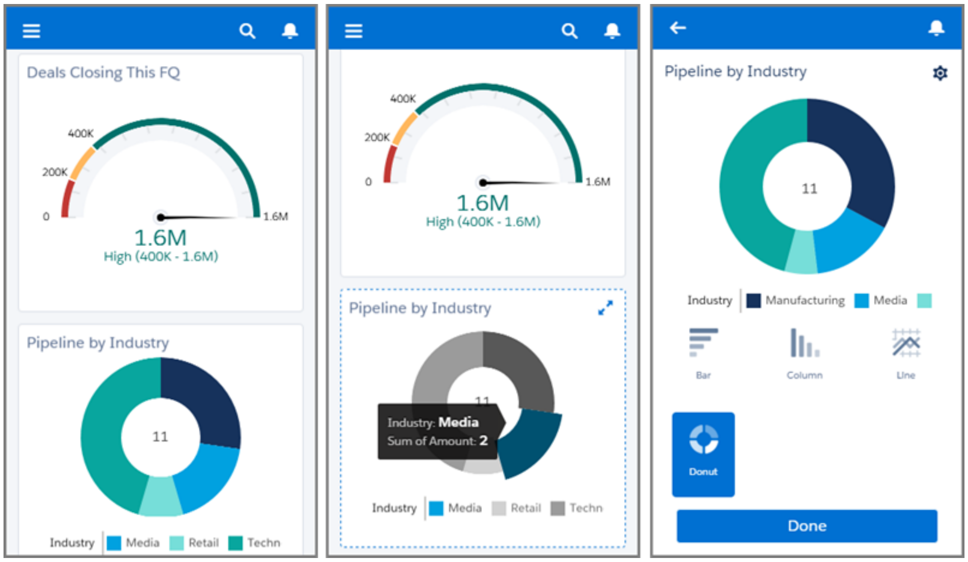
Available in: Enhanced Folder Sharing and Legacy Folder Sharing

USER PERMISSIONS

To modify report and dashboard settings:

- **Legacy Folder Sharing**
  Run Reports AND Manage Dashboards

  Enhanced Folder Sharing
  Manage Reports



After you enable enhanced charts, everyone sees them in the Salesforce app regardless of whether they use Lightning Experience or Salesforce Classic on the full Salesforce site.

1. From Setup, enter `Reports and Dashboards Settings` in the `Quick Find` box, then select **Reports and Dashboards Settings**.
2. Select **Enable Enhanced Charts in Salesforce**.
3. Click **Save**.

Before enabling enhanced charts, take note of these limitations:

- Except for line and bar charts, which display up to 500 groups, Enhanced Charts show only the first 200 groups.
- On tablets, dashboards always have two columns. On phones, dashboards always have one column.
- On mobile dashboards, Enhanced Chart components don't show footers, but titles and subtitles still display. If there is important information in a component footer, consider moving it to the title or subtitle.
- You can’t share metric, gauge, or table charts in Chatter.
- Enhanced Charts have a different color palette than Legacy Charts.

Let Users Subscribe to Report Notifications

Allow users to subscribe to reports to be notified whenever certain metrics meet conditions they specify.

1. From Setup, enter `Report Notifications` in the `Quick Find` box, then select **Report Notifications**.
2. Select the option to enable report notifications.
3. Click **Save**.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

Customize Report and Dashboard Email Notifications

Choose how users are notified when information changes in the reports and dashboards they use.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

1. From Setup, enter *`Email Notifications`* in the `Quick Find` box, then select **Email Notifications**.
2. Select or clear the following options to modify the notifications for your organization:

   Allow Reports and Dashboards to Be Sent to Portal Users

   If you enable this option, all internal and portal users specified as recipients receive reports and dashboards. If this option isn't enabled, only internal Salesforce users can receive reports and dashboard refresh notifications.

   This option, disabled by default, is available to Enterprise, Unlimited, and Performance Edition organizations that have a Customer Portal or partner portal set up.

   `Use Images Compatible with Lotus Notes in Dashboard Emails`

   Dashboard refresh notifications can be sent to specified users when a scheduled dashboard refresh completes. By default, Salesforce sends images in dashboard emails as `.png` (Portable Network Graphic) files, which are not supported in Lotus Notes. When you enable the `Use Images Compatible with Lotus Notes in Dashboard Emails` > option, Salesforce uses `.jpg` images, which Lotus Notes supports, when sending dashboard emails. The "Schedule Dashboard" permission is required to view this option.

   Note: Dashboard emails that contain images compatible with Lotus Notes are substantially larger and the image quality can be lower.

3. Click **Save**.

Set Up a Custom Report Type

A *report type* defines the set of records and fields available to a report based on the relationships between a primary object and its related objects. Reports display only records that meet the criteria defined in the report type.

For example, an administrator can create a report type that shows only job applications that have an associated resume; applications without resumes won't show up in reports using that type. An administrator can also show records that *may* have related records—for example, applications with or without resumes. In this case, all applications, whether or not they have resumes, are available to reports using that type.

You can create custom report types from which users can report on your organization's reports and dashboards. When defining a custom report type, select Reports or Dashboards from the `Primary Object` drop-down list on the New Custom Report Type page.

Tip: When you're done creating your report type, consider ways you can do more with it:

- Add the custom report type to apps you upload to Force.com AppExchange.
- Users designated as a translator with the "View Setup and Configuration" permission can translate custom report types using the Translation Workbench.

IN THIS SECTION:

1. Create a Custom Report Type

   Choose the primary object you'd like your new report type to support, then give it a name and a useful description. Mark it as "in development" until you're ready to make it available for users to create reports.

2. Add Child Objects To Your Custom Report Type

   To enable reports to pull data from more than just the primary object, consider adding one or more related objects to your report type.

3. Design the Field Layout for Reports Created From Your Custom Report Type

   After you define a custom report type and choose its object relationships, you can specify the standard and custom fields a report can display when created or run from a custom report type.

4. Manage Custom Report Types

   After you create a custom report type, you can customize, edit, and delete it.

5. Limits on Report Types

   Custom report types are subject to some limits to ensure high performance and usability.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Available in: Enhanced Folder Sharing and Legacy Folder Sharing

USER PERMISSIONS

To create and update custom report types:

- **Legacy Folder Sharing**

  Create and Customize Reports

  AND

  Manage Custom Report Types

  Enhanced Folder Sharing

  Create and Customize Reports

  AND

  Manage Custom Report Types

To delete custom report types:

- **Legacy Folder Sharing**

  Create and Customize Reports

  AND

  Manage Custom Report Types

  Enhanced Folder Sharing

  Create and Customize Reports

  AND

  Manage Custom Report Types

Create a Custom Report Type

Choose the primary object you'd like your new report type to support, then give it a name and a useful description. Mark it as "in development" until you're ready to make it available for users to create reports.

1. From Setup, enter `Report Types` in the `Quick Find` box, then select **Report Types**.
2. Click **New Custom Report Type**.
3. Select the `Primary Object` for your custom report type.

   Tip:

   - You can choose from all objects—even those you don't have permission to view. This lets you build report types for a variety of users.
   - Once you save a report type, you can't change the primary object.
   - If the primary object on a report type is a custom or external object, and that object is deleted, the report type and reports created from it are deleted.
   - If you remove an object from a report type, all references to that object and its associated objects are removed from the reports and dashboards based on that type.

4. Enter the `Report Type Label` and the `Report Type Name`.

   The label can be up to 50 characters long. The name is used by the SOAP API.

5. Enter a description for your custom report type, up to 255 characters long.

   Provide a meaningful description so users have a good idea of which data is available for reports. For example: *`Accounts with Contacts. Report on accounts and their contacts. Accounts without contacts are not shown.`*.

6. Select the category in which you want to store the custom report type.
7. Select a `Deployment Status`:
   - Choose `In Development` during design and testing as well as editing. The report type and its reports are hidden from all users except those with the "Manage Custom Report Types" permission. Only users with that permission can create and run reports using report types in development.
   - Choose `Deployed` when you''re ready to let all users access the report type.

   Note: A custom report type's `Deployment Status` changes from `Deployed` to `In Development` if its primary object is a custom or external object whose `Deployment Status` similarly changes.

8. Click **Next**.

A developer can edit a custom report type in a managed package after it's released, and can add new fields. Subscribers automatically receive these changes when they install a new version of the managed package. However, developers can't remove objects from the report type after the package is released. If you delete a field in a custom report type that's part of a managed package, and the deleted field is part of bucketing or used in grouping, you receive an error message.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Available in: Enhanced Folder Sharing and Legacy Folder Sharing

USER PERMISSIONS

To create and update custom report types:

- **Legacy Folder Sharing**
  Create and Customize Reports

  AND

  Manage Custom Report Types

  Enhanced Folder Sharing
  Create and Customize Reports

  AND

  Manage Custom Report Types

To delete custom report types:

- **Legacy Folder Sharing**
  Create and Customize Reports

  AND

  Manage Custom Report Types

  Enhanced Folder Sharing
  Create and Customize Reports

  AND

  Manage Custom Report Types

Add Child Objects To Your Custom Report Type

To enable reports to pull data from more than just the primary object, consider adding one or more related objects to your report type.

1. Click the box under the primary object.
2. Select a child object.

   Only related objects are shown.

   Tip: Type in the search box to find objects quickly.

3. For each child object, select one of the following criteria:
   - `Each "A" record must have at least one related "B" record.` Only parent records with child records are shown in the report.
   - `"A" records may or may not have related "B" records.` Parent records are shown, whether or not they have child records.

   When Users are the primary object, select child objects by field—for example, Accounts (Account Owner) or Accounts (Created By).

4. Add up to three child objects.

   The number of children depends on the objects you choose.

5. Click **Save**.

Example:

- If you select that object A may or may not have object B, then all subsequent objects automatically include the may-or-may-not association on the custom report type. For example, if accounts are the primary object and contacts are the secondary object, and you choose that accounts may or may not have contacts, then any tertiary and quaternary objects included on the custom report type default to may-or-may-not associations.
- Blank fields display on report results for object B when object A does not have object B. For example, if a user runs a report on accounts with or without contacts, then contact fields display as blank for accounts without contacts.
- On reports where object A may or may not have object B, you can't use the OR condition to filter across multiple objects. For example, if you enter filter criteria *`Account Name starts with M OR Contact First Name starts with M`*, an error message displays informing you that your filter criteria is incorrect.
- The `Row Limit` option on tabular reports shows only fields from the primary object on reports created from custom report types where object A may or may not have object B. For example, in an accounts with or without contacts report, only fields from accounts are shown. Fields from objects after a may-or-may-not association on custom report types aren't shown. For example, in an accounts with contacts with or without cases report, only fields from accounts and contacts are available to use. Also, existing reports may not run or disregard the `Row Limit` settings if they were created from custom report types where object associations changed from object A with object B to object A with or without object B.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Available in: Enhanced Folder Sharing and Legacy Folder Sharing

USER PERMISSIONS

To create and update custom report types:

- **Legacy Folder Sharing**

  Create and Customize Reports

  AND

  Manage Custom Report Types

  Enhanced Folder Sharing

  Create and Customize Reports

  AND

  Manage Custom Report Types

To delete custom report types:

- **Legacy Folder Sharing**

  Create and Customize Reports

  AND

  Manage Custom Report Types

  Enhanced Folder Sharing

  Create and Customize Reports

  AND

  Manage Custom Report Types

Design the Field Layout for Reports Created From Your Custom Report Type

After you define a custom report type and choose its object relationships, you can specify the standard and custom fields a report can display when created or run from a custom report type.

Note: Custom fields appear in custom report types only if they've been added to that report type's page layout.

1. From Setup, enter `Report Types` in the `Quick Find` box, then select **Report Types** to display the All Custom Report Types page.
2. Select the custom report type you want to edit and click **Edit Layout** on the Fields Available for Reports section.

   You can click **Preview Layout** to preview which fields will display on the Select Columns page of a report customized or run from this report type.

   Note: When previewing the layout, all fields and objects are displayed, including fields and objects you may not have permission to access. However, you cannot access any data stored in the fields or objects that you do not have permission to access.

3. Select fields from the right-hand box and drag them to a section on the left.

   Tip: You can view a specific object's fields by selecting an object from the `View` drop-down list.

4. Optionally, click **Add fields related via lookup** to display the Add Fields Via Lookup overlay.

   From here you can add fields via the lookup relationship the object selected in the `View` drop-down list has to other objects.

   - A lookup field is a field on an object that displays information from another object. For example, the `Contact Name` field on an account.
   - A custom report type can contain fields available via lookup through four levels of lookup relationships. For example, for an account, you can get the account owner, the account owner's manager, the manager's role, and that role's parent role.
   - You can only add fields via lookup that are associated with objects included in the custom report type. For example, if you add the accounts object to the custom report type, then you can add fields from objects to which accounts have a lookup relationship.
   - Selecting a lookup field on the Add Fields Via Lookup overlay may allow you to access additional lookup fields from other objects to which there is a lookup relationship. For example, if you select the `Contact Name` field from cases, you can then select the `Account` field from contacts because accounts have a lookup relationship to contacts which have a lookup relationship to cases.
   - The fields displayed in the Add Fields Via Lookup overlay do not include lookup fields to primary objects. For example, if accounts are the primary object on your custom report type, and contacts are the secondary object, then the Add Fields Via Lookup overlay does not display lookup fields from contacts to accounts.
   - Fields added to the layout via the **Add fields related via lookup** link are automatically included in the section of the object from which they are a lookup field. For example, if you add the `Contact` field as a lookup from accounts, then the `Contact` field is automatically included in the Accounts section. However, you can drag a field to any section.
   - Fields added via lookup automatically display the lookup icon on the field layout of the custom report type.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Available in: Enhanced Folder Sharing and Legacy Folder Sharing

USER PERMISSIONS

To create and update custom report types:

- **Legacy Folder Sharing**

  Create and Customize Reports

  AND

  Manage Custom Report Types

  Enhanced Folder Sharing

  Create and Customize Reports

  AND

  Manage Custom Report Types

To delete custom report types:

- **Legacy Folder Sharing**

  Create and Customize Reports

  AND

  Manage Custom Report Types

  Enhanced Folder Sharing

  Create and Customize Reports

  AND

  Manage Custom Report Types

- Reduce the amount of time it takes a user to find fields to report on by grouping similar fields together on custom report types' field layouts. You can create new page sections in which to group fields that are related to one another, and you can group fields to match specific detail pages and record types.
- If you include activities as the primary object on a custom report type, then you can only add lookup fields from activities to accounts on the select column layout of the custom report type.

5. Arrange fields on sections as they should appear to users.

   Fields not dragged onto a section will be unavailable to users when they generate reports from this report type.

6. Click **Preview Layout** and use the legend to determine which fields are included on the layout, added to the report by default, and added to the layout via a lookup relationship.

   Warning: Users can view roll-up summary fields on reports that include data from fields they do not have access to view. For example, a user that does not have access to view the `Price` field on an opportunity product can view the `Total Price` field on opportunity reports if he or she has access to the `Total Price` field.

7. To rename or set which fields are selected by default for users, select one or more fields and click **Edit Properties**.
   - Click the `Checked by Default` checkbox next to one or more fields.

     Fields selected by default automatically display the checkbox icon (✓) on the field layout of the custom report type.

   - Change the text in the `Display As` field next to the field you want to rename.

     Note: Renamed fields from standard objects, as well as renamed standard objects, do not display as such on the field layout of the custom report type. However, renamed fields from standard objects and renamed standard objects do display their new names on the report and the preview page, which you can access by clicking **Preview Layout**.

8. To rename the sections, click **Edit** next to an existing section, or create a new section by clicking **Create New Section**.
9. Click **Save**.

Manage Custom Report Types

After you create a custom report type, you can customize, edit, and delete it.

From Setup, enter `Report Types` in the `Quick Find` box, then select **Report Types** to display the All Custom Report Types page, which shows the list of custom report types defined for your organization.

- Select a list view from the `View` drop-down list to go directly to that list page, or click **Create New View** to define your own custom view.
- Define a new custom report type by clicking **New Custom Report Type**.
- Update a custom report type's name, description, report type category, and deployment status by clicking **Edit** next to a custom report type's name.
- Delete a custom report type by clicking **Del** next to the custom report type's name. All the data stored in the custom report type will be deleted and cannot be restored from the Recycle Bin.

  > Important: When you delete a custom report type, any reports based on it are also deleted. Any dashboard components created from a report based on a deleted custom report type display an error message when viewed.

- Display detailed information about a custom report type and customize it further by clicking a custom report type's name.

  After you click a custom report type name you can:

  - Update which object relationships a report can display when run from the custom report type.
  - Edit the page layout of the custom report type to specify which standard and custom fields a report can display when created or run from the custom report type.
  - See how the fields display to users in reports run from the custom report type by clicking **Preview Layout** on the Fields Exposed for Reporting section.
  - Create a new custom report type with the same object relationships and fields as the selected custom report type by clicking **Clone**.
  - Rename fields in the report.
  - Set which fields are selected by default.

When you edit a report, you can see the report type displayed above the report name in report builder. The report type isn't displayed on the report run page.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Available in: Enhanced Folder Sharing and Legacy Folder Sharing

USER PERMISSIONS

To create and update custom report types:

- **Legacy Folder Sharing**
  Create and Customize Reports

  AND

  Manage Custom Report Types

  Enhanced Folder Sharing
  Create and Customize Reports

  AND

  Manage Custom Report Types

To delete custom report types:

- **Legacy Folder Sharing**
  Create and Customize Reports

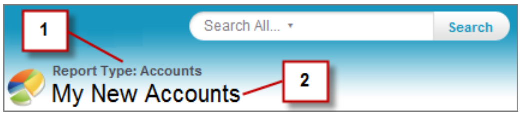
  AND

  Manage Custom Report Types

  Enhanced Folder Sharing
  Create and Customize Reports

  AND

  Manage Custom Report Types



1. Report type
2. Report name

Note: If the Translation Workbench is enabled for your organization, you can translate custom report types for international users.

Limits on Report Types

Custom report types are subject to some limits to ensure high performance and usability.

- You can add up to 1000 fields to each custom report type. A counter at the top of the Page Layout step shows the current number of fields included. If you have too many fields, you can't save the layout.
- You can't add the following fields to custom report types:
  - Product schedule fields
  - History fields
  - Person account fields
  - The `Age` field on cases and opportunities
- A custom report type can contain up to 60 object references. For example, if you select the maximum limit of four object relationships for a report type, then you could select fields via lookup from an additional 56 objects. However, users will receive an error message if they run a report from a custom report type and the report contains columns from more than 20 different objects.
- Object references can be used as the main four objects, as sources of fields via lookup, or as objects used to traverse relationships. Each referenced object counts toward the maximum limit even if no fields are chosen from it. For example, if you do a lookup from account to account owner to account owner's role, but select no fields from account owner, all the referenced objects still count toward the limit of 60.
- Reports run from custom report types that include cases do not display the `Units` drop-down list, which allows users to view the time values of certain case fields by hours, minutes, or days.
- You can't add forecasts to custom report types.
- Report types associated with custom objects in the Deleted Custom Objects list count against the maximum number of custom report types you can create.

Turn On Enhanced Folder Sharing for Reports and Dashboards

When you enable folder sharing, Salesforce converts your users' existing folder access levels to use new, more detailed access levels.

Note: If your organization was created after the Summer '13 Salesforce release, you already have enhanced folder sharing. If your organization existed before the Summer '13 release, follow these steps to make folder sharing available to your users.

When enhanced sharing is in effect, all users in the organization get Viewer access by default to report and dashboard folders that are shared with them. Users might have more access if they are Managers or Editors on a given folder, or if they have more administrative user permissions. Each user's access to folders under the new capability is based on the combination of folder access and user permissions they had before enhanced folder sharing was enabled.

1. From Setup, enter `Folder Sharing` in the `Quick Find` box, then select **Folder Sharing**.
2. Select **Enable access levels for sharing report and dashboard folders**.
3. Click **Save**.

Important: If you go back to the old folder sharing model, existing report and dashboard folders go back to the state they were in before.

- If a folder existed before enhanced folder sharing was enabled, its properties and sharing settings are rolled back to their previous state.
- If a folder was created while enhanced enhanced folder sharing was in effect, it is hidden from the folder list and all its sharing settings are removed. Administrative user permissions are still in effect.

EDITIONS

Available in: Salesforce Classic

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

Available in: Legacy Folder Sharing

USER PERMISSIONS

To view the enhanced folder sharing setting:

- View Dashboards in Public Folders AND View Reports in Public Folders

To modify the enhanced folder sharing setting:

- Edit My Dashboards and Edit My Reports

Set Up Historical Trend Reporting

To make historical trend reports available to your users, start by using filters to configure the amount of data that's captured for historical trend reporting. Then select the fields needed for historical reports.

Shape your historical trend data to have enough for users to exploit but doesn't exceed the space limits. Consider which fields contain useful historical data and which fields contain data you can leave out.

Important: Retaining historical data increases the amount of data you store. The effect depends on the ways your organization works. Say that someone updates the status of a typical opportunity record every day or two. Historical trending data for the Status field on the Opportunity object takes up more space than if the record changes once or twice a month. If any of your trended objects is in danger of exceeding the data limit, you receive an email alert.

1. From Setup, enter `Historical Trending` in the `Quick Find` box, then select **Historical Trending**.
2. Select the object that you want to do historical trend reporting on.

   You can select Opportunities, Cases, Forecasting Items, and up to 3 custom objects. Historical trend reporting is available only for Collaborative forecasting, not Customizable forecasting. If Cumulative Forecast Rollups are enabled in Collaborative Forecasts settings, Forecasting Items are not available in historical trend reports.

3. Select **Enable Historical Trending**.
4. Use the filters under **Configure Data** to specify the total amount of data you can use to create historical trend reports.

   You can narrow down historical data for Opportunities, Cases, and custom objects. For Forecasting Items, the available data is selected for you.

For example, to reduce the data stored for Opportunities reports, drop out the least likely deals by setting `Stage not equal to Prospecting`.

5. Under **Select Fields**, choose up to 8 fields to make available for historical trend reporting.

   These fields can be selected when creating historical trending reports.

   - For Opportunities reporting, 5 fields are preselected: Amount, Close Date, Forecast Category, Probability, and Stage. You can add 3 more.
   - For Forecasting, all 8 available fields are pre-selected.

After you enable historical trending, a new custom report type is available when you create future reports. If you enable historical trending on a new field, that field is automatically added to the historical trending report layout.

When you turn off historical trending, keep these points in mind.

- Turning off historical trending for a field hides the historical data for that field. If you re-enable historical trending, historical data for the field can be viewed again, including data created after historical trending was turned off.
- Turning off historical trending for an object causes all historical data and configuration settings to be deleted for that object. The object's historical trending report type and any reports that have been created with it are also deleted.
- If you turn off historical trending for a field and delete it, the field's historical data is no longer available even if you re-enable historical trending.

Note:

- The historical fields available to each user depend on the fields that user can access. If your permissions change and you can no longer see a given field, that field's historical data also becomes invisible.
- Each historical field has the same field-level security as its parent field. If the field permissions for the parent field change, the historical field's permissions change accordingly.

SEE ALSO:

Tip Sheet: Historical Trend Reporting for Opportunities

Upgrade the Report Wizard

Report builder, a powerful drag-and-drop editor, is the standard tool for creating and editing reports. If your organization is still using the old report wizard, you should upgrade to report builder.

- All profiles get access to the report builder by default. (You may continue to see the “Report Builder” permission in permission sets and profiles and the PermissionSet and Profile objects in the API, though the upgrade overrides those settings.)
- The old report wizard is available only to users in Accessibility Mode.
- Group and Professional Edition organizations can use report builder.
- You get scatter charts, a new chart type for reports.

New organizations automatically get the latest version of report builder. If you don't see the Report Builder Upgrade section on the User Interface Settings page, the upgrade has already been enabled for your organization.

Assigning the “Report Builder” permission or the “Report Builder (Lightning Experience)” permission to all users through profiles or permission sets isn't the same thing as enabling report builder for your entire organization. To enable report builder for your organization, follow these steps.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To modify report and dashboard settings:

- Customize Application

Important: Upgrading **does not affect** any of your existing reports. However, once you upgrade, you can't return to the old report wizard.

1. From Setup, enter `Reports` in the `Quick Find` box, then select **Reports and Dashboards Settings**.
2. Check **Enable Lightning Report Builder (Beta)**.
3. Review the Report Builder Upgrade section of the page and click **Enable**. If you don't see the button, report builder has already been enabled for your entire organization.
4. Confirm your choice by clicking **Yes, Enable Report Builder for All Users**.
5. Click **Save**.

Respond to Critical Updates

EDITIONS

Available in: Lightning Experience and Salesforce Classic

Available in: All Editions

Salesforce periodically releases updates that improve the performance, logic, and usability of Salesforce, but may affect your existing customizations. When these updates become available, Salesforce lists them in Setup at **Critical Updates** and displays a message when administrators go to Setup.

To ensure a smooth transition, each update has an opt-in period during which you can manually activate and deactivate the update an unlimited number of times to evaluate its impact on your organization and modify affected customizations as necessary. The opt-in period ends on the auto-activation date, at which time Salesforce permanently activates the update.

Warning: Salesforce recommends testing each update by activating it in either your Developer Sandbox or your production environment during off-peak hours.

To manage critical updates, from Setup, click **Critical Updates**. From this page, you can view the summary, status, and auto-activation date for any update that Salesforce has not permanently activated. To view more details about the update, including a list of customizations in your organization that the update might affect, click **Review**.

If an update has an **Activate** link, click it to test the update in your sandbox or production environment before Salesforce automatically activates it.

Notes on Critical Updates

- Salesforce analyzes your organization to determine if a critical update potentially affects your customizations. If your customizations are not affected, Salesforce automatically activates the update in your organization.
- On the scheduled auto-activation date, Salesforce permanently activates the update. After auto-activation, you cannot deactivate the update.
- Each update detail page describes how your customizations might be affected and how you can correct any unintended functionality.
- Salesforce displays a message the first time you access the setup menu after a critical update becomes available. The message lets you choose to have Salesforce display the updates immediately or remind you about the updates later.

Organize Data with Divisions

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

Note: Divisions do not restrict access to data and are not meant for security purposes.

EDITIONS

Available in: Salesforce Classic

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

IN THIS SECTION:

How Divisions Work

Divisions can be assigned to users and other kinds of records. For example, you can create a report to show the opportunities for just the North American division to get accurate sales numbers for the North American sales team.

Set Up Divisions

When setting up divisions, you must create divisions and assign records to divisions to make sure that your data is categorized effectively.

Create and Edit Divisions

Creating logical divisions for your organization helps you segment your records to make searching and reporting easier.

Transferring Multiple Records Between Divisions

Select groups of records to move into or between divisions.

Change the Default Division for Users

If you can manage user settings, you can change a user's default division.

Reporting With Divisions

If your organization uses divisions to segment data, you can customize your reports to show records within specific divisions.

SEE ALSO:

Administrator tip sheet: Getting Started with Divisions

How Divisions Work

Divisions can be assigned to users and other kinds of records. For example, you can create a report to show the opportunities for just the North American division to get accurate sales numbers for the North American sales team.

EDITIONS

Available in: Salesforce Classic

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

- **Record-level division**—Division is a field on individual records that marks the record as belonging to a particular division. A record can belong to a division created by the administrator or the standard "global" division. The standard global division is created automatically when your organization enables divisions. A record can belong to only one division at a time.
- **Default division**—Users are assigned a default division that applies to their newly created accounts, leads, and custom objects that are enabled for divisions.
- **Working division**—If you have the "Affected by Divisions" permission, you can set the division using a drop-down list in the sidebar. Then, searches show only the data for the current working division. You can change your working division at any time. If you don't have the "Affected by Divisions" permission, you always see records in all divisions.

The following table shows how using divisions affects different areas.

Area	Description
Search	If you have the "Affected by Divisions" permission: • In sidebar search, you can select a single division, or all divisions. • In advanced search, you can select a single division or all divisions. • In global search, you can search a single division or all divisions. • For searches in lookup dialogs, the results include records in the division you select from the drop-down list in the lookup dialog window. Note: All searches within a specific division also include the global division. For example, if you search within a division called Western Division, your results include records found in both the Western Division and the global division. If you do not have the "Affected by Divisions" permission, your search results always include records in all divisions.
List views	If you have the "Affected by Divisions" permission, list views include only the records in the division you specify when creating or editing the list view. List views that don't include all records (such as My Open Cases) include records in all divisions. If you do not have the "Affected by Divisions" permission, your list views always include records in all divisions.
Chatter	Chatter doesn't support divisions. For example, you can't use separate Chatter feeds for different divisions.
Reports	If you have the "Affected by Divisions" permission, you can set your report options to include records in just one division or all divisions. Reports that use standard filters (such as My Cases or My team's accounts) show records in all divisions, and can't further limited to a specific division. If you do not have the "Affected by Divisions" permission, your reports always include records in all divisions.
Viewing records and related lists	When viewing the detail page of a record, the related lists show all associated records that you have access to, regardless of division.
Creating records	When you create accounts, leads, or custom objects that are enabled for divisions, the division is automatically set to your default division, unless you override this setting. When you create records related to an account or other record that already has a division, the new record is assigned to the existing record's division. For example, if you create a custom object record that is on the detail side of a master-detail relationship with a custom object that has divisions enabled, it is assigned the master record's division.

Area	Description
	When you create records that are not related to other records, such as private opportunities or contacts not related to an account, the division is automatically set to the global division.
Editing records	When editing accounts, leads, or custom objects that are enabled for divisions, you can change the division. All records that are associated through a master-detail relationship are automatically transferred to the new division as well. For example, contacts and opportunities are transferred to the new division of their associated account. Detail custom objects are transferred to their master record's new division. When editing other types of records, you can't change the division setting.
Custom objects	When you enable divisions for a custom object, Salesforce initially assigns each record for that custom object to the global division. When you create a custom object record: • If the custom object is enabled for divisions, the record adopts your default division. • If the custom object is on the detail side of a master-detail relationship with a divisions-enabled custom object, the record adopts the division of the master record.
Relationships	If you convert a lookup relationship to a master-detail relationship, detail records lose their current division and inherit the division of their master record. If you convert a master-detail relationship to a lookup relationship, the previous master record determines the division for any detail records. If you delete a master-detail relationship, the previous master record determines the division for any detail records.

Set Up Divisions

When setting up divisions, you must create divisions and assign records to divisions to make sure that your data is categorized effectively.

Before you can use the divisions feature for your organization, you must enable divisions. If you are using a standard object, contact Salesforce to enable divisions for your organization. For custom objects, select `Enable Divisions` on the custom object definition page to enable divisions.

1. Plan which divisions you need based on how you want to segment your data.
   For example, use one division for all the records belonging to your North American sales team and one division for your European sales team.

   100

2. Create divisions for your organization. All existing records are assigned to the "Global" division by default. You can change the default division name, create more divisions, and move user and data records between divisions.
3. Transfer leads, accounts, and custom objects into relevant divisions. When records are assigned to a division, associated records are assigned the same division.
   For example, when you change the division assigned to an account, related records such as contacts and opportunities are assigned to the same division.
4. Add division fields to page layouts.
5. Add divisions to field-level security.
6. Set the default division for all users. New accounts and leads are assigned to the user's default division unless the user explicitly assigns a different division. New records related to existing records are assigned to the existing record's division.
7. Enable the "Affected by Divisions" permission for users.

   Users with this permission can limit list views by division, search within a division, or report within a division. Users who don't have the "Affected by Divisions" permission still have a default user-level division. They can view division fields, change the division for a record, and specify a division when creating records.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To create or edit divisions:
- Modify All Data

Create and Edit Divisions

Creating logical divisions for your organization helps you segment your records to make searching and reporting easier.

Divisions must be enabled for the organization.

All records are initially assigned to the default "Global" division until the user defines the division. You can create up to 100 divisions, including any inactive ones.

1. From Setup, enter *`Manage Divisions`* in the `Quick Find` box, then select **Manage Divisions**.
2. To create a division, click **New**, or **Edit** change an existing division.
3. Enter the division name.
4. To make the division active, select the checkbox.

   Note: You can't deactivate a division if users or lead queues are assigned to that division.

5. Click **Save**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create or edit divisions:
- Modify All Data

6. To change the order that divisions appear in the Divisions picklist, click **Sort**. Then to use the arrow buttons to move divisions higher or lower in the list.

Transferring Multiple Records Between Divisions

Select groups of records to move into or between divisions.

To reassign the divisions for multiple records at one time, transfer groups of accounts, leads, or users between divisions.

1. From Setup, enter *`Mass Division Transfer`* in the `Quick Find` box, then select **Mass Division Transfer**.
2. Select the type of record you want to transferred, then click **Next**. When you change the division assigned to an account, related records such as contacts and opportunities are assigned to the same division. When you change the division assigned to a custom object, other custom objects belonging to it are also transferred to the new division.
3. Select search conditions that records must match and click **Next**.
4. Select the division you want to transfer the records to.
5. If you're transferring user records, you can select `Change the division...` to also transfer the users' records to the new division.
6. Click **Transfer**. You'll receive an email notification when the transfer is complete. If 5,000 or more records are being transferred, the request will be placed in a queue for processing.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To mass transfer records:
- Modify All Data

Change the Default Division for Users

If you can manage user settings, you can change a user's default division.

If your organization uses divisions to segment data, a default division is assigned to all users and is applied to new accounts, leads, and appropriate custom objects .The default division doesn't prevent users from viewing or creating records in other divisions. If, however, the new record is related to an existing record, the new record is assigned the same division as the existing record.

1. From Setup, enter *`Users`* in the `Quick Find` box, then select **Users**.
2. Click the name, alias, or username of the user whose default division you want to change.
3. Next to the `Default Division` field, click **Change**.
4. Select a new default division.
5. Select an action to be applied to records the user already owns.
6. Click **Save**.

If you are changing your own default division, skip step 1 and go to your personal settings. Enter *`Advanced User Details`* in the `Quick Find` box, then select **Advanced User Details**.No results? Enter *`Personal Information`* in the `Quick Find` box, then select **Personal Information**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To change a user's default division:
- Manage Users

Reporting With Divisions

If your organization uses divisions to segment data, you can customize your reports to show records within specific divisions.

Use the Division drop-down list on the report to select one of the following.

- A specific division
- Your current working division.
- All records across all divisions.

Note: Reports that use standard filters (such as My Cases or My Team's Accounts) show records in all divisions. These reports can't be further limited to a specific division.

SEE ALSO:

Change Your Working Division

Personalize Your Salesforce Experience

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Available in: Enhanced Folder Sharing and Legacy Folder Sharing

USER PERMISSIONS

To create, edit, and delete reports:

- **Legacy Folder Sharing**
  Create and Customize Reports

  AND

  Report Builder

  Enhanced Folder Sharing
  Create and Customize Reports

  AND

  Report Builder

Salesforce Upgrades and Maintenance

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

IN THIS SECTION:

Read-Only Mode

Access to your data at a moment's notice—even during our planned maintenance windows. To minimize interruption to your business, Salesforce gives users read-only access during splits, instance migrations, instance switches, pre-scripts, and certain other maintenance events.

5 Minute Upgrades

Salesforce reserves just five minutes of scheduled maintenance time to roll out new major versions of our service. These upgrades to the next release occur three times per year.

Check for Desktop Client Updates

Read-Only Mode

EDITIONS

Available in: **All Editions**

Access to your data at a moment's notice—even during our planned maintenance windows. To minimize interruption to your business, Salesforce gives users read-only access during splits, instance migrations, instance switches, pre-scripts, and certain other maintenance events.

What to Expect in Read-Only Mode

When Salesforce is in read-only mode, you can navigate within the application and view and report on your business data.

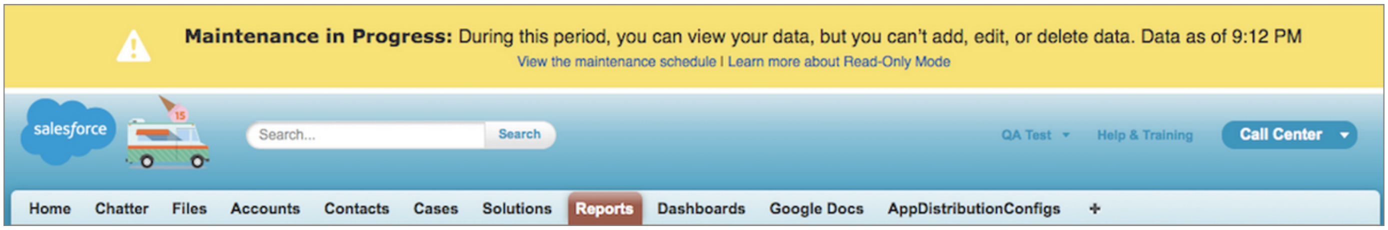
During read-only mode, you **can't**:

- Add, edit, or delete data
- Perform any actions in Salesforce that modify your Salesforce data. For example:
  - Post on Chatter
  - Use LiveAgent
  - Refresh dashboards
  - Perform API write or edit actions
  - Perform bulk API read actions
  - Save new or edited reports

    Note: You can still run existing reports.

Activity reminders don't occur, and Recent Items lists don't update. Login history is still recorded for compliance purposes, but it isn't reflected in your organization until a few minutes after the organization exits read-only mode.

When your organization is in read-only mode, desktop and mobile browser users see a banner at the top of their browser window:



Maintenance in Progress: During this period, you can view your data, but you can't add, edit, or delete data. Data as of 9:12 PM

View the maintenance schedule | Learn more about Read-Only Mode

When to Expect Read-Only Mode

The maintenance schedule posted on trust.salesforce.com indicates whether each upcoming maintenance window includes read-only access. Planned maintenance windows vary in length depending on the level of maintenance needed. In addition, when users are notified two weeks before a planned maintenance window, the notification specifies whether the maintenance includes read-only access.

If you'd like to see how your organization works in read-only mode, contact Salesforce to have the testing option enabled in your sandbox organization.

5 Minute Upgrades

Salesforce reserves just five minutes of scheduled maintenance time to roll out new major versions of our service. These upgrades to the next release occur three times per year.

Although your organization should expect to experience a disruption of up to five minutes, the interruption is typically one minute or less. Users receive an error message letting them know that the service is unavailable during the upgrade, and are prompted to log in again when the upgrade is complete.

EDITIONS

Available in: Salesforce Classic

Available in all editions

Check for Desktop Client Updates

Desktop clients such as Salesforce for Outlook and Connect Offline integrate Salesforce with your PC. Your administrator controls which desktop clients you are allowed to install.

If your administrator enabled Home tab alerts, an alert banner displays on your Home tab when a new client version is available.

You can also see which clients are installed on your computer and check for updates on your own.

1. From your personal settings, enter *`Check for Updates`* in the `Quick Find` box, then select **Check for Updates**.
2. From the table, review the names and version numbers of available desktop clients.
3. If you are using Internet Explorer, click the correct desktop client and then click **Install Now** to install a client. If you are using another browser such as Mozilla Firefox, click **Download Now** to save the installer file to your computer. To run the installer program, double-click the saved file.

After you install the update, the alert banner displays on your Home tab until you log in through the newly updated client.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To view client update alerts:

- On, updates w/alerts

  OR

  On, must update w/alerts

  on your profile

Permissions for UI Elements, Records, and Fields

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

What you can view or edit also depends on how you customized your personal display or page layout and what edition your org is using. This table described the different access levels in more detail.

EDITIONS

Available in: Salesforce Classic

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

Action	Access Needed
To view a tab:	You must have the “Read” permission on the records within that tab. If you don’t see a particular tab, verify that you customized your personal display to show the tab.
To view a record:	You must have the “Read” permission on the type of record you want to view.

Action	Access Needed
	If you can't view a certain record, check whether your org uses a sharing model or territory management. In certain sharing models, the owner of the record has to specifically share the record to grant view access to others. Territory management can restrict access to accounts, opportunities, and cases.
To view a field:	You must have the "Read" permission on the type of record for the field. If you can't view a certain field, check field-level security and your page layout. Field-level security can restrict access to a field. Page layouts can hide fields.
To edit a field:	You must have the "Edit" permission on the type of record for the field. If you can't edit a certain field, check field-level security and your page layout. Field-level security can restrict access to a field. Page layouts can set fields to not be editable.
To view a related list:	You must have the "Read" permission on the type of records displayed in the related list. If you can't view a certain field, check your page layout. Page layouts can hide fields.
To view a button or link:	Make sure that you have the necessary permission to perform the action. Buttons and links only display for users who have the appropriate user permissions to use them.

How Do I Discontinue Service?

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

Users who are up-to-date with their payments can request a complete download of the data in the system.

To submit your request directly, contact the Salesforce Customer Support Billing Department.

User Management

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

The available user management options vary according to which Salesforce Edition you have.

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

Important: Salesforce recommends that you appoint a backup administrator for your org. A backup administrator can keep your org running in case your primary administrator is unavailable.

As an administrator, you perform user management tasks, such as:

- Create and edit users
- Reset passwords
- Create Google Apps accounts
- Grant permissions
- Create and manage other types of users
- Create custom fields
- Set custom links
- Run reports on users
- Delegate user administration tasks to other users

Depending on your Salesforce edition and the additional features that your company purchased, you have specific licenses, such as Marketing or Connect Offline. The licenses let users access features that are not included in their user licenses. You can assign one or more of these licenses to users and also set up accounts for users outside your org to access a limited set of fields and objects. You can grant access to the Customer Portal, partner portal, or Self-Service through user licenses. Using Salesforce to Salesforce, create connections to share records with other Salesforce users outside of your org.

Note: Starting with Spring '12, the Self-Service portal isn't available for new orgs. Existing orgs continue to have access to the Self-Service portal.

IN THIS SECTION:

View and Manage Users

In the user list, you can view and manage all users in your org, partner portal, and Salesforce Customer Portal.

Licenses Overview

To enable specific Salesforce functionality for your users, you must choose one user license for each user. To enable additional functionality, you can assign permission set licenses and feature licenses to your users or purchase usage-based entitlements for your organization.

Passwords

Salesforce provides each user in your organization with a unique username and password that must be entered each time a user logs in. As an administrator, you can configure several settings to ensure that your users' passwords are strong and secure.

Control Login Access

Control whether your users are prompted to grant account access to Salesforce admins, and whether users can grant access to publishers.

Log In as Another User

To assist other users, administrators can log in to Salesforce as another user. Depending on your organization settings, individual users might need to grant login access to administrators.

Delegate Administrative Duties

Use delegated administration to assign limited admin privileges to users in your org who aren't administrators. For example, let's say you want the Customer Support team manager to manage users in the Support Manager role and all subordinate roles. Create a delegated admin for this purpose so that you can focus on other administration tasks.

Topics and Tags Settings

When you enable topics for objects, users can add topics to records so they can quickly retrieve related items using list views. With Chatter enabled, users can also see related items on the Records tab of each topic detail page. Enabling topics for an object disables public tags on records of that object type. Personal tags aren't affected.

SEE ALSO:

View and Manage Users

Licenses Overview

View and Manage Users

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Customer Portal and partner portals are not available in **Database.com**

USER PERMISSIONS

To view user lists:

- View Setup and Configuration

In the user list, you can view and manage all users in your org, partner portal, and Salesforce Customer Portal.

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

From the user list, you can:

- Create one user.
- Create multiple users.
- Reset passwords for selected users.
- Edit a user.
- View a user's detail page by clicking the name, alias, or username.
- View or edit a profile by clicking the profile name.
- If Google Apps™ is enabled in your org, export users to Google and create Google Apps accounts by clicking **Export to Google Apps**.

Note: You can perform many of these tasks from the SalesforceA mobile app.

Tips for Managing Users

- Create custom fields for users and set custom links to display on the user detail page. To access these options, go to the object management settings for users.
- Use the sidebar search to search for any user in your org, regardless of the user's status. When using a lookup dialog from fields within records, the search results return only active users. You can also run user reports in the Reports tab.
- To simplify user management in orgs with many of users, delegate aspects of user administration to non-administrator users.

  Note: You cannot delegate administrative duties related to your org to partner portal or Customer Portal users. However, you can delegate some portal administrative duties to portal users.

IN THIS SECTION:

Guidelines for Adding Users

Understand important options for adding users. Learn what to communicate to users about passwords and logging in.

Administrators and Separation of Duties

Separating duties limits the power of any one person or entity so that you can help prevent a single point of failure. For example, you can have two or more administrators who have responsibilities for administering different portions of your org. If you have only one administrator, consider assigning a backup person to the role. You can give the backup person the same profile or permission set that your primary administrator has.

Add a Single User

Depending on the size of your organization or your new hire onboarding process, you may choose to add users one at a time. The maximum number of users you can add is determined by your Salesforce edition.

Add Multiple Users

You can quickly add up to 10 users at a time to your organization. Your Salesforce edition determines the maximum number of users that you can add.

Edit Users

To change user details—such as a user's profile, role, or contact information—edit the user account.

Unlock Users

Users can be locked out of an organization if they enter incorrect login credentials too many times. Unlock users to restore their access.

Deactivate (Delete) Users

You can't delete a user, but you can deactivate an account so a user can no longer log in to Salesforce.

Freeze or Unfreeze User Accounts

In some cases, you can't immediately deactivate an account, such as when a user is selected in a custom hierarchy field. To prevent users from logging in to your organization while you perform the steps to deactivate them, you can freeze user accounts.

Restrict User Email Domains

You can define a whitelist to restrict the email domains allowed in a user's `Email` field.

User Fields

The fields that comprise the Personal Information and other personal settings pages describe a user.

Salesforce Adoption Manager

Quickly turn your mobile employees into Salesforce power users with Salesforce Adoption Manager. This tool trains and engages your users with intelligent email journeys aimed at driving adoption of the Salesforce app and Lightning Experience. After inviting users to download the mobile app, Adoption Manager follows up with tips that help users get the most out of Salesforce. It also encourages dormant Salesforce users to try using the app again.

SEE ALSO:

Deactivate (Delete) Users

Freeze or Unfreeze User Accounts

Help Users From Anywhere With SalesforceA

Guidelines for Adding Users

Understand important options for adding users. Learn what to communicate to users about passwords and logging in.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

- Your username must be unique across all Salesforce orgs. The username must be in the format of an email address, for example, jane@salesforce.com. The email used for your username doesn't have to function. You can have the same email address associated with your account across multiple orgs. Remember: The username in the form of an email address must remain unique.
- If your name includes non-English characters and you use Outlook, add the specified language to the mail format settings within Outlook.
- The account verification link emailed to new users expires in six months, and users have to change their password the first time they log in. Users who click the account verification link but don't set a password need an admin to reset their password before they can log in.
- Not all options are available for all license types. For example, the Marketing User and Allow Forecasting options aren't available for Force.com user licenses because the Forecasts and Campaigns tabs aren't available to Force.com license users. Force.com user licenses are not available for Professional, Group, or Contact Manager Editions.
- In Performance, Unlimited, Enterprise, and Developer Edition orgs, you can select **Send Apex Warning Emails**. This option sends an email to the user when an application that invokes Apex uses more than half of the resources specified by the governor limits. You can use this feature during Apex code development to test the amount of resources used at runtime.
- You can move users between profiles based on user licenses that have the same record sharing models. For example, you can move a Force.com-based profile user to a Salesforce-based profile or vice versa. The user sometimes loses permission access depending on what the user licenses permit. If you move a user with permission set assignments, the user is removed from the permission set. If you try to add the user back to the permission set, you receive a licensing error, unless the new license allows the permissions.

SEE ALSO:

Add a Single User

Administrators and Separation of Duties

Administrators and Separation of Duties

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

The availability of each permission set license depends on the edition requirements for permission sets and the related feature.

Separating duties limits the power of any one person or entity so that you can help prevent a single point of failure. For example, you can have two or more administrators who have responsibilities for administering different portions of your org. If you have only one administrator, consider assigning a backup person to the role. You can give the backup person the same profile or permission set that your primary administrator has.

While the practice of having one person perform all administrative duties can make sense, it can lead to troubles. For example, what if:

- Your administrator falls ill, and a mission-critical change must be made to your org.
- Your administrator left your company on unhappy terms but is the only person who has the administrator profile credentials.

Prevent possible problems by ensuring that more than one person can perform key administrative tasks. Depending on which edition you use, you can create a custom profile cloned from the Administrator profile. Then assign the cloned profile to an appropriate person. If you can't clone profiles, consider implementing a process to ensure business continuity if your sole administrator is unavailable. You can also delegate administration tasks by assigning a delegated administrator.

SEE ALSO:

Add a Single User

Delegate Administrative Duties

Add a Single User

Depending on the size of your organization or your new hire onboarding process, you may choose to add users one at a time. The maximum number of users you can add is determined by your Salesforce edition.

1. Read the guidelines for adding users.
2. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.
3. Click **New User**.
4. Enter the user's name and email address and a unique username in the form of a email address. By default, the username is the same as the email address.

   Important: Your username must be unique across all Salesforce orgs. The username must be in the format of an email address, for example, jane@salesforce.com. The email used for your username doesn't have to function. You can have the same email address associated with your account across multiple orgs. Remember: The username in the form of an email address must remain unique.

5. In Professional, Enterprise, Unlimited, Performance, and Developer Editions, select a `Role`.
6. Select a `User License`. The user license determines which profiles are available for the user.
7. Select a profile, which specifies the user's minimum permissions and access settings.
8. If your organization has Approvals enabled, you can set the user's approver settings, such as delegated approver, manager, and preference for receiving approval request emails.
9. Check `Generate new password and notify user immediately` to have the user's login name and a temporary password emailed to the new user.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create users:

- Manage Internal Users

SEE ALSO:

Guidelines for Adding Users

Add Multiple Users

Edit Users

User Fields

Licenses Overview

Add Multiple Users

You can quickly add up to 10 users at a time to your organization. Your Salesforce edition determines the maximum number of users that you can add.

1. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.
2. Click **Add Multiple Users**.
3. If multiple user license types are available in your organization, select the user license to associate with the users you plan to create. The user license determines the available profiles.
4. Specify the information for each user.
5. To email a login name and temporary password to each new user, select **Generate passwords and notify user via email**.
6. Click **Save**.
7. To specify more details for the users that you've created with this method, edit individual users as needed.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create users:

- Manage Internal Users

SEE ALSO:

Add a Single User

Edit Users

User Fields

Licenses Overview

Edit Users

To change user details—such as a user's profile, role, or contact information—edit the user account.

1. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.
2. Click **Edit** next to a user's name.
3. Change the settings as needed.
4. Click **Save**.

Tip: You can perform this and other administration tasks from the SalesforceA mobile app.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit users:

- Manage Internal Users

IN THIS SECTION:

Considerations for Editing Users

Be aware of the following behaviors when editing users.

SEE ALSO:

User Fields

Unlock Users

Help Users From Anywhere With SalesforceA

Considerations for Editing Users

Be aware of the following behaviors when editing users.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Usernames

A username must be unique across all Salesforce organizations. It must use the format of an email address (such as xyz@abc.org), but doesn't need to be a real email address. While users can have the same email address across organizations, usernames must be unique.

If you change a username, a confirmation email with a login link is sent to the email address associated with that user account. If an organization has multiple login servers, sometimes users can't log in immediately after you've changed their usernames. The change can take up to 24 hours to replicate to all servers.

Changing email addresses

If `Generate new password and notify user immediately` is disabled when you change a user's email address, Salesforce sends a confirmation message to the email address that you entered. Users must click the link provided in that message for the new email address to take effect. This process ensures system security.

Personal information

Users can change their personal information after they log in.

User sharing

If the organization-wide default for the user object is Private, users must have Read or Write access to the target user to access that user's information.

Domain names

You can restrict the domain names of users' email addresses to a list of specific domains. Any attempt to set an email address with another domain results in an error message. To enable this functionality for your organization, contact Salesforce.

SEE ALSO:

Edit Users

Unlock Users

Users can be locked out of an organization if they enter incorrect login credentials too many times. Unlock users to restore their access.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To unlock users:
- Manage Internal Users

1. From Setup, enter *`Users`* in the `Quick Find` box, then select **Users**.
2. Select the locked user.
3. Click **Unlock**.

   This button appears only when a user is locked out.

Tip: You can perform this and other administration tasks from the SalesforceA mobile app.

SEE ALSO:

Edit Users

Set Password Policies

Help Users From Anywhere With SalesforceA

Deactivate (Delete) Users

You can't delete a user, but you can deactivate an account so a user can no longer log in to Salesforce.

Watch a Demo: ▶ Removing Users' Access to Salesforce (Salesforce Classic—English only)

1. From Setup, enter *Users* in the `Quick Find` box, then select **Users**.
2. Click **Edit** next to a user's name.
3. Deselect the `Active` checkbox and then click **Save**.

Tip: You can perform this and other administration tasks from the SalesforceA mobile app.

IN THIS SECTION:

Considerations for Deactivating Users

Be aware of the following behaviors when deactivating users.

SEE ALSO:

Freeze or Unfreeze User Accounts

Mass Transfer Records

Help Users From Anywhere With SalesforceA

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To deactivate users:
- Manage Internal Users

Considerations for Deactivating Users

Be aware of the following behaviors when deactivating users.

User licenses and billing

A deactivated user doesn't count against your organization's available user licenses. However, deactivating a user doesn't reduce the number of licenses for which your organization is billed. To change your billing, you must change your organization's license count.

Users in custom hierarchy fields

You can't deactivate a user that's selected in a custom hierarchy field even if you delete the field. To deactivate a user in a custom hierarchy field, delete and permanently erase the field first.

Workflow email alert recipients

You can't deactivate a user that's assigned as the sole recipient of a workflow email alert.

Customer Portal Administrator users

You can't deactivate a user that's selected as a Customer Portal `Administrator`.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Record access

Deactivated users lose access to any records that were manually shared with them, or records that were shared with them as team members. Users higher in the role hierarchy relative to the deactivated users also lose access to those records. However, you can still transfer their data to other users and view their names on the Users page.

Note: If your organization has Asynchronous Deletion of Obsolete Shares (Pilot) enabled, removal of manual and team shares is run during off-peak hours between 6 PM and 4 AM based on your organization's default time zone. For account records, manual and team shares are deleted right after user deactivation.

Deactivated users lose access to shared records immediately. Users higher in the role hierarchy continue to have access until that access is deleted asynchronously. If that visibility is a concern, remove the record access that's granted to the deactivated users before deactivation.

Chatter

If you deactivate users in an organization where Chatter is enabled, they're removed from Following and Followers lists. If you reactivate the users, the subscription information in the Following and Followers lists is restored.

If you deactivate multiple users, subscription information isn't restored for users that follow each other. For example, user A follows user B and user B follows user A. If you deactivate users A and B, their subscriptions to each other are deleted from Following and Followers lists. If user A and user B are then reactivated, their subscriptions to each other aren't restored.

Salesforce Files

Files owned by a deactivated user are not deleted. The deactivated user is the file owner until an admin reassigns the files to an active user. Files shared in a content library can be edited by other library members with author or delete permissions. Sharing rules remain active until an admin modifies them.

`Created By` fields

It's possible for inactive users to be listed in `Created By` fields even when they're no longer active in an organization. This happens because some system operations create records and toggle preferences, acting as an arbitrary administrator user to complete the task. This user can be active or inactive.

Accounts and opportunities owned by deactivated users

You can create and edit accounts, opportunities, and custom object records that are owned by inactive users. For example, you can edit the `Account Name` field on an opportunity record that's owned by an inactive user. To enable this feature, contact Salesforce.

Territories and forecasting

Deactivated users continue to own opportunities and appear in forecasts and territories. When users are deactivated, their opportunity forecast overrides, adjusted total overrides, and manager's choice overrides on subordinates' forecasts are frozen. However, the manager of a deactivated user can apply manager's choice overrides to that user's forecasts. Rollup amounts are kept current. If a deactivated user is later reactivated, the user can resume normal work as before. If "Allow Forecasting" is disabled for a user who is deactivated, the user is removed from any territories he or she is assigned to.

Opportunity and account teams

Deactivated users are removed from the default opportunity and account teams of other users. The deactivated users' default opportunity and account teams are not removed.

Account teams

If a user on an account team has Read/Write access (**Account Access**, **Contact Access**, **Opportunity Access**, and **Case Access**) and is deactivated, the access will default to Read Only if the user is reactivated.

Opportunity teams

If you deactivate users in an organization where opportunity splitting is enabled, they aren't removed from any opportunity teams where they're assigned a split percentage. To remove a user from an opportunity team, first reassign the split percentage.

Delegated external user administrators

When a delegated external user admin deactivates a portal user, the admin doesn't have the option to remove the portal user from teams that user is a member of.

SEE ALSO:

Deactivate (Delete) Users

Freeze or Unfreeze User Accounts

In some cases, you can't immediately deactivate an account, such as when a user is selected in a custom hierarchy field. To prevent users from logging in to your organization while you perform the steps to deactivate them, you can freeze user accounts.

Let's say a user just left your company. You want to deactivate the account, but the user is selected in a custom hierarchy field. Because you can't immediately deactivate the account, you can freeze it in the meantime.

Tip: You can perform this and other administration tasks from the SalesforceA mobile app.

1. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.
2. Click the username of the account you want to freeze.
3. Click **Freeze** to block access to the account or **Unfreeze** to allow access to the account again.

Note: Freezing user accounts doesn't make their user licenses available for use in your organization. To make their user licenses available, deactivate the accounts.

SEE ALSO:

Deactivate (Delete) Users

Troubleshoot Login Issues

Help Users From Anywhere With SalesforceA

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To freeze or unfreeze user accounts:

- Manage Users

Restrict User Email Domains

You can define a whitelist to restrict the email domains allowed in a user's `Email` field.

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

   Note: If you don't see this page, contact your Salesforce representative to enable it.

2. Click **New Allowed Email Domain**.
3. Enter a `Domain`.

   You can enter a top-level domain, such as *`sampledoc.org`*, or a subdomain, such as *`emea.sampledoc.org`*.

4. Click **Save**.

You can repeat the steps to add more email domains to the whitelist.

Once you've added one or more whitelisted email domains, the `Email` field for each new user must match a whitelisted domain.

The `Email` field for existing users doesn't have to comply with the whitelist. However, if you edit an existing user, update the `Email` field to match a whitelisted email domain.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To restrict user email domains:

- Manage Users

Note: The email domain whitelist doesn't apply to users external to your organization, such as portal, Communities, or Chatter External users.

SEE ALSO:

- Add a Single User
- Add Multiple Users
- Edit Users

User Fields

EDITIONS

Available in: Salesforce Classic and Lightning Experience

The fields that comprise the Personal Information and other personal settings pages describe a user.

The visibility of fields depends on the specific page, your org's permissions, and your Salesforce edition.

Field	Description
`Accessibility Mode`	When selected, enables a user interface mode designed for visually impaired users.
`Active`	Administrative checkbox that enables or disables user login to the service.
`Address`	Street address for user. Up to 255 characters are allowed in this field.
`Alias`	Short name to identify the user on list pages, reports, and other pages where the entire name does not fit. Up to 8 characters are allowed in this field.
`Allow Forecasting`	Indicates whether the user can use customizable forecasting.
`Api Token`	Indicates whether an API token has been reset. If issues occur, Salesforce uses this field to help you troubleshoot issues related to API tokens.
`App Registration: One-Time Password Generator`	When connected, the user can verify identity with a code from an authenticator app other than Salesforce Authenticator, such as Google Authenticator. For example, the user enters a code from the app when logging in from an IP address outside the company's trusted IP range. This type of verification code is sometimes called a time-based one-time password, or TOTP. Users with Two-Factor Authentication for User Interface Logins permission need to use a second factor of authentication when logging in to Salesforce through the user interface. A

Field	Description
	current verification code generated by the authenticator app counts as a second factor. If the user has Two-Factor Authentication for API Logins permission and connects an authenticator app, the user enters the current code from the app to access the service. The user doesn't enter the standard security token.
`App Registration: Salesforce Authenticator`	When connected, the user can verify identity by responding to a push notification with the Salesforce Authenticator mobile app, version 2 or later. For example, the user approves a notification when logging in from an IP address outside the company's trusted IP network. If the user sets a trusted location in the app and is allowed to use location-based automated verifications, Salesforce Authenticator can automatically verify the user's identity from that trusted location. Users can connect both Salesforce Authenticator and another authenticator app to the same Salesforce account. When connected, the user can also verify identity with a code from Salesforce Authenticator. For example, the user enters a code from the app when logging in from an IP address outside the company's trusted IP network. This type of verification code is sometimes called a time-based one-time password, or TOTP. Users with Two-Factor Authentication for User Interface Logins permission need to use a second factor of authentication when logging in to Salesforce through the user interface. A manual or automated response to a notification from Salesforce Authenticator counts as a second factor. If the user has Two-Factor Authentication for API Logins permission and connects Salesforce Authenticator, the user enters the current code from the app to access the service. The user doesn't enter the standard security token.
`Call Center`	The name of the call center to which this user is assigned.
`Checkout Enabled`	Indicates whether the user is notified by email when the user's Checkout account is activated and available for login. Enabling this option requires the Manage Billing permission.
`City`	City portion of user's address. Up to 40 characters are allowed in this field.
`Color-Blind Palette on Charts`	Indicates whether the option to set an alternate color palette for charts has been enabled. The alternate palette has been optimized for use by color-blind users. For dashboard emails, the alternate palette is not used.
`Company`	Company name where user works. Up to 40 characters are allowed in this field.

Field	Description
`Contact`	Name of the associated contact if the user is a partner user.
`Country`	Country portion of user's address. Entry is selected from a picklist of standard values, or entered as text. Up to 80 characters are allowed if the field is a text field.
`Created By`	User who created the user including creation date and time. (Read only)
`Currency`	User's default currency for quotas, forecasts, and reports. Shown only in orgs using multiple currencies. This currency must be one of the active currencies for the org.
`Custom Links`	Listing of custom links for users as set up by your administrator.
`Data.com User Type`	Enables a user to find contact and lead records from Data.com and add them to Salesforce. Also indicates the type of Data.com user. Data.com Users get a limited number of account, contact, and lead records to add or export per month, and their unused additions expire at the end of each month. Data.com List Users get a limited number of account, contact, and lead records to add or export per month, and their unused additions expire at the end of each month. After the monthly limit is used, List Users draw record additions from a pool that is shared by all List Users in the organization. Unused pool additions expire one year from purchase.
`Default Currency ISO Code`	User's default currency setting for new records. Available only for orgs that use multiple currencies.
`Default Division`	Division that is applied, by default, to all new accounts and leads created by the user, unless the user explicitly sets a different division. When users create records related to an account or other record that already has a division, the new record is assigned to the existing record's division. The default division is not used. This setting does not restrict the user from viewing or creating records in other divisions. Users can override change their default division at any time by setting a working division. Available only in orgs that use divisions to segment their data.
`Delegated Approver`	User lookup field used to select a delegate approver for approval requests. Depending on the approval process settings, this user can also approve approval requests for the user.
`Department`	Group that user works for, for example, Customer Support. Up to 80 characters are allowed in this field.
`Development Mode`	Enables development mode for creating and editing Visualforce pages. This field is visible only to orgs that have Visualforce enabled.

Field	Description
`Disable Auto Subscription For Feeds`	Disables automatic feed subscriptions to records owned by a user. Only available in orgs with Chatter enabled.
`Division`	Company division to which user belongs for example, PC Sales Group. Up to 40 characters are allowed in this field.
`Email`	Email address of user. Must be a valid email address in the form: jsmith@acme.com. Up to 80 characters are allowed in this field.
`Email Encoding`	Character set and encoding for outbound email sent by user from within Salesforce. English-speaking users use ISO-8859-1, which represents all Latin characters. UTF-8 (Unicode) represents characters for all languages, however some older email software doesn't support it. Shift_JIS, EUC-JP, and ISO-2022-JP are useful for Japanese users.
`Employee Number`	Identifying number for a user.
`End of day`	Time of day that user generally stops working. Used to define the times that display in the user's calendar.
`Fax`	Fax number for user.
`Federation ID`	The value used to identify a user for federated authentication single sign-on.
`First Name`	First name of user, as displayed on the user edit page. Up to 40 characters are allowed in this field.
`Force.com Flow User`	Grants the ability to run flows. Available in Developer (with limitations), Enterprise, Unlimited, and Performance Editions. Enabling this option requires the Manage Force.com Flow permission. If the user has the Run Flows permission, don't enable this field.
`Force.com Quick Access Menu`	Enables the Force.com quick access menu, which appears in object list view and record detail pages. The menu provides shortcuts to customization features for apps and objects.
`Information Currency`	The default currency for all currency amount fields in the user record. Available only for orgs that use multiple currencies.
`Knowledge User`	Grants access to Salesforce Knowledge. The user's profile determines whether the user has access to the Article Management tab or Articles tab. Available in Professional, Enterprise, Unlimited, and Performance Editions.
`Language`	The primary language for the user. All text and online help is displayed in this language. In Professional, Enterprise, Unlimited, and Performance Edition orgs, a user's individual Language setting overrides the org's Default Language.

Field	Description
	Not available in Personal Edition, Contact Manager, or Group Edition™. The org's Display Language applies to all users.
`Last Login`	The date and time when the user last successfully logged in. This value is updated if 60 seconds have elapsed since the user's last login. (Read only)
`Last Name`	Last name of user, as displayed on the user edit page. Up to 80 characters are allowed in this field.
`Last Password Change or Reset`	The date and time of this user's last password change or reset. This read-only field appears only for users with the Manage Users permission.
`Lightning Login`	Allows the user to enroll in and use Lightning Login, for password-free logins. The Enroll option indicates that a Salesforce admin has given the user the option to enroll. The Cancel option indicates that the user has enrolled, and can cancel their enrollment if needed.
`Locale`	Country or geographic region in which user is located. The `Locale` setting affects the format of date, date/time, and number fields, and the calendar. For example, dates in the English (United States) locale display as 06/30/2000 and as 30/06/2000 in the English (United Kingdom) locale. Times in the English (United States) locale display using a twelve-hour clock with AM and PM (for example, 2:00 PM), whereas in the English (United Kingdom) locale, they're displayed using a 24-hour clock (for example, 14:00). The `Locale` setting also affects the first and last name order on `Name` fields for users, leads, and contacts. For example, Bob Johnson in the English (United States) locale displays as Bob Johnson, whereas the Chinese (China) locale displays the name as Johnson Bob. For Personal Edition users, the locale is set at the org level (from Setup, enter *`Company Information`* in the Quick Find box, then select **Company Information**). For all other users, their personal locale, available at their personal information page, overrides the org setting.
`Make Setup My Default Landing Page`	When this option is enabled, users land in the Setup page when they log in.
`Manager`	Lookup field used to select the user's manager. This field: • Establishes a hierarchical relationship, preventing you from selecting a user that directly or indirectly reports to itself. • Allows Chatter to recommend people and records to follow based on your org's reporting structure.

Field	Description
	This field is especially useful for creating hierarchical workflow rules and approval processes without creating more hierarchy fields. Note: Unlike other hierarchy fields, you can inactivate users referenced in the Manager field.
`Marketing User`	When enabled and the user has Read permission on contacts or the Import permission on Leads, and Edit permission on campaigns, the user can create, edit, and delete campaigns, configure advanced campaign setup, and add campaign members and update their statuses with the Data Import Wizard. Available in Professional, Enterprise, Unlimited, and Performance Editions. If this option isn't selected, or the user doesn't have the necessary permissions, the user can only view campaigns and advanced campaign setup, edit the Campaign History for a single lead or contact, and run campaign reports.
`Middle Name`	Middle name of the user, as displayed on the user edit page. Up to 40 characters are allowed for this field. Note: To enable this field, contact Salesforce Customer Support. Next, from Setup, enter *`User Interface`* in the Quick Find box, then select **User Interface**. Then select **Enable Name Suffixes for Person Names**.
`Mobile`	Cellular or mobile phone number. Up to 40 characters are allowed in this field. This number is used for SMS-based identity confirmation. Administrators enable SMS-based identity confirmation from Setup by entering *`Session Settings`* in the Quick Find box, then selecting **Session Settings**, and then selecting the **Enable the SMS method of identity confirmation** option. After the SMS method of identity confirmation is enabled, users without a verified mobile number in their profiles are asked after logging in to register for mobile verification. This process applies to users without mobile numbers. Users can take one of the following actions. • Enter a mobile phone number and then have it verified with a text message containing a verification code. • Skip entering a mobile number now, but be asked again at the next login. • Opt out of mobile verification. Users who select this action can register a mobile number later in their personal information. Chatter Free and Chatter External license users who select this action need an administrator to set the mobile number.

Field	Description
	After a user's mobile phone number is verified, Salesforce uses it to authenticate the user when necessary. For example, verification occurs when a user logs in from an unknown IP address. Administrators can also enter users' mobile numbers and pre-verify them. If **Enable the SMS method of identity confirmation** is enabled when an administrator enters a mobile number for a user, or when a mobile number is set from an API using the `User` object, the mobile number is considered verified. If **Enable the SMS method of identity confirmation** is not enabled, the new mobile phone number is not considered verified.
`Mobile Configuration`	The mobile configuration assigned to the user. If no mobile configuration is specified, this field defaults to the mobile configuration assigned to the user's profile. This field is visible to orgs that use Salesforce to manage mobile configurations.
`Mobile User`	Allocates one Salesforce Mobile Classic license to the user, granting the user access to Salesforce Mobile Classic app. The number of user records enabled by this checkbox can't exceed the total number of mobile licenses your org has. Available in Professional, Enterprise, Unlimited, and Performance Editions. The Mobile User option is enabled by default for Unlimited, Performance, and Developer Edition users. To prevent users from activating the Salesforce Mobile Classic app on their mobile devices before you're ready to deploy it, disable this option for all users. If users have already activated their Salesforce Mobile Classic account, deselecting the Mobile User option revokes the user's mobile license. The next time the user's device synchronizes with Salesforce, all the Salesforce data is deleted from the device, and the device is no longer associated with the user.
`Modified By`	User who last changed the user fields, including modification date and time. (Read only)
`Monthly Contact and Lead Limit`	If the user's Data.com User Type is Data.com User, the number of Data.com contact and lead records the user can add each month. The default number of records per license is 300, but you can assign more or fewer, up to the org limit.
`Name`	Combined first name, middle name (beta), last name, and suffix (beta) of user, as displayed on the user detail page.
`Nickname`	A nickname is the name used to identify this user in a community. Up to 40 alphanumeric characters are allowed. Standard users can edit this field.

Field	Description
`Offline User`	Administrative checkbox that grants the user access to Connect Offline. Available in Professional, Enterprise, Unlimited, and Performance Editions.
`Partner Super User`	Denotes whether a partner portal user is a super user.
`Phone`	Phone number of user. Up to 40 characters are allowed in this field.
`Profile`	Administrative field that specifies the user's base-level permissions to perform different functions within the application. You can grant more permissions to a user through permission sets.
`Receive Approval Request Emails`	Preference for receiving approval request emails. This preference also affects whether the user receives approval request notifications in the Salesforce app or Lightning Experience.
`Receive Salesforce CRM Content Daily Digest`	Specifies that non-portal users with a Salesforce CRM Content User license and Salesforce CRM Content subscription receive a daily email summary if activity occurs on their subscribed content, libraries, tags, or authors. To receive email, you must also select the `Receive Salesforce CRM Content Email Alerts` option. Portal users do not need the Salesforce CRM Content User license. They need only the View Content in Portals user permission.
`Receive Salesforce CRM Content Email Alerts`	Specifies that non-portal users with a Salesforce CRM Content User license and Salesforce CRM Content subscription receive email notifications if activity occurs on their subscribed content, libraries, tags, or authors. To receive real-time email alerts, select this option and do not select the `Receive Salesforce CRM Content Daily Digest` option. Portal users do not need the Salesforce CRM Content User license. They need only the View Content in Portals user permission.
`Role`	Administrative field that specifies position of user within an organization, for example, Western Region Support Manager. Roles are selected from a picklist of available roles, which the administrator can change. Not available in Personal Edition, Contact Manager, or Group Edition.
`Salesforce CRM Content User`	Indicates whether a user can use Salesforce CRM Content. Available in Professional, Enterprise, Unlimited, and Performance Editions.
`Salesforce App User`	Turns on automatic redirection to the Salesforce mobile web when a user logs in to Salesforce from a supported mobile Web browser. The Salesforce mobile web option must be enabled for your org.

Field	Description
`Self-Registered via Customer Portal`	When enabled, specifies that the user was created via self-registration to a Customer Portal. Available in Enterprise, Unlimited, and Performance Editions.
`Security Key (U2F)`	Allows the user to register and use a U2F security key as a second factor of authentication. The Register option indicates that a Salesforce admin has given users in the org the option to register a security key. The Remove option indicates that the user has registered a security key, and can remove their registration if needed.
`Send Apex Warning Emails`	Specifies that users receive an email notification whenever they execute Apex that surpasses more than 50 percent of allocated governor limits. Available in Developer, Enterprise, Unlimited, and Performance Editions only.
`Show View State in Development Mode`	Enables the View State tab in the development mode footer for Visualforce pages. This field is only visible to orgs that have Visualforce enabled and **Development Mode** selected.
`Site.com Contributor User`	Allocates one Site.com Contributor license to the user, granting the user limited access to Site.com Studio. Users with a Contributor license can use Site.com Studio to edit site content only. The number of user records with this checkbox enabled can't exceed the total number of Site.com Contributor licenses your org has. Available in Developer, Enterprise, Unlimited, and Performance Editions, only if Site.com is enabled for your org.
`Site.com Publisher User`	Allocates one Site.com Publisher license to the user, granting the user full access to Site.com Studio. Users with a Publisher license can build and style websites, control the layout and functionality of pages and page elements, and add and edit content. The number of user records with this checkbox enabled can't exceed the total number of Site.com Publisher licenses your org has. Available in Developer, Enterprise, Unlimited, and Performance Editions, only if Site.com is enabled for your org.
`Start of day`	Time of day that user generally starts working. Used to define the times that display in the user's calendar.
`State/Province`	State or province portion of user's address. Entry is selected from a picklist of standard values, or entered as text. Up to 80 characters are allowed if the field is a text field.

Field	Description
`Suffix`	Name suffix of the user, as displayed on the user edit page. Up to 40 characters are allowed for this field. Note: To enable this field, contact Salesforce Customer Support. Next, from Setup, enter *`User Interface`* in the Quick Find box, then select **User Interface**. Then select **Enable Name Suffixes for Person Names**.
`Temporary Verification Code`	Users can enter a temporary code when they lose the device that they usually use for two-factor authentication. Only Salesforce admins can generate or expire a temporary code for a user. Users can expire their own code.
`Time Zone`	Primary time zone in which user works. Users in Arizona should select the setting with **America/Phoenix**, and users in parts of Indiana that do not follow Daylight Savings Time should select the setting with **America/Indianapolis**.
`Title`	Job title of user. Up to 80 characters are allowed in this field.
`Used Space`	Amount of disk storage space the user is using.
`User License`	Indicates the type of user license.
`Username`	Administrative field that defines the user's login. Up to 80 characters are allowed in this field.
`Zip/Postal Code`	Zip code or postal code portion of user's address. Up to 20 characters are allowed in this field.

SEE ALSO:

View and Manage Users

User Licenses

View Your Organization's Feature Licenses

Restrict User Email Domains

Salesforce Adoption Manager

Quickly turn your mobile employees into Salesforce power users with Salesforce Adoption Manager. This tool trains and engages your users with intelligent email journeys aimed at driving adoption of the Salesforce app and Lightning Experience. After inviting users to download the mobile app, Adoption Manager follows up with tips that help users get the most out of Salesforce. It also encourages dormant Salesforce users to try using the app again.

Important: By undertaking the role of Salesforce admin, you represent and warrant to us that you have the necessary consent and authorization from your users to allow us to send email or text messages to them (which may include commercial or promotional emails and text messages) based on their usage of Salesforce.

Is Salesforce Adoption Manager Available for All Orgs?

Adoption Manager is currently available for orgs in the United States, the U.K., and Australia. Adoption Manager determines your country by the billing country for your Salesforce account. All new Salesforce orgs start with Adoption Manager enabled by default. Note that Adoption Manager is not available for customers on the NA21 instance of Salesforce.

What Kind of Results Can I Expect from Salesforce Adoption Manager?

With customized tips and feedback, this program is designed to help you and your users get more out of Salesforce. For example, by using the Salesforce app effectively, customers report amazing results:

- 40% increase in employee satisfaction
- 29% faster time to find information
- 26% increase in sales productivity

Does Enabling Salesforce Adoption Manager Change the Usage of User Data?

The only change when you enable Salesforce Adoption Manager is that your users receive email messages from the program, based on their usage of Salesforce on page 212. You can review our privacy statement for more details.

What Happens After I Activate Salesforce Adoption Manager for My Users?

After you activate the program, Salesforce Adoption Manager begins targeting content for users regarding the Salesforce app and Lightning Experience. All emails are optimized for desktop and mobile devices.

If users access the email from a desktop, they can text a link to download Salesforce to their mobile devices. After users download Salesforce, they receive emails based on their actual usage of the mobile app. These emails suggest top actions to take and also keep track of actions already taken. The goal is to get users up to speed with Salesforce so your company can start realizing more benefits from the product.

Salesforce Adoption Manager also helps your users capture the power of Lightning Experience by highlighting key Lightning features that drive productivity and help close deals faster.

Will My Users Get Notifications or Other Types of Messages in Addition to Emails?

Initially, Salesforce Adoption Manager sends email messages only. We plan to add mobile notifications in the future so users can get the tips they need while using Salesforce.

What Do the Emails from Salesforce Adoption Manager Look Like?

Check out this video to see for yourself!

Can I Customize the Content of the Salesforce Adoption Manager Emails?

No.

Who Receives the Salesforce Adoption Manager Emails? How Frequently Are Emails Sent Out?

Emails are delivered to users with full Salesforce licenses only. Community, Partner, and Chatter users aren’t included.

Adoption Manager is intelligent about who receives emails.

- The invitation to download Salesforce is sent only to users who have permission to access the mobile app and have not yet installed the app.
  - Five separate tips are sent to all users who downloaded Salesforce within the last 60 days.
  - A single reminder to use Salesforce is sent to users who haven't accessed the mobile app for 30 days.
- The invitation to try Lightning Experience is sent only to users enabled for Lightning.

Are Salesforce Adoption Manager Emails Counted Against My Org's Limits?

No. The emails are sent from Salesforce Marketing Cloud servers instead of from your org.

How Can I Confirm That Salesforce Adoption Manager Emails Are Actually Going Out?

Contact Salesforce Customer Support for more information.

Can I Configure Salesforce Adoption Manager to Send Emails to a Specific Group of Users Only?

No. When you enable Adoption Manager, it's turned on for all users in your org. But users can opt out of receiving future messages from the footer of any email from the program.

Can Users Opt Back into Receiving Salesforce Adoption Manager Emails After Opting Out?

Yes. The first Adoption Manager email includes a link that allows users to opt back into receiving future emails. Consider encouraging your users to save this email, just in case.

If I Turn on Salesforce Adoption Manager, Can I Opt Out Later?

Yes. As the Admin of the org, you are opting in your users to receive Adoption Manager emails. To opt your users out, from Setup in the full Salesforce site, enter *`Adoption`* in the `Quick Find` box, select **Adoption Manager**, and then deselect `Enable Salesforce Adoption Manager`.

SEE ALSO:

Salesforce App

Get the Salesforce App

Licenses Overview

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Edition requirements vary for each user, permission set, and feature license type.

To enable specific Salesforce functionality for your users, you must choose one user license for each user. To enable additional functionality, you can assign permission set licenses and feature licenses to your users or purchase usage-based entitlements for your organization.

Specific features in Salesforce require specific permissions. For example, to view cases, a user must have the "Read" permission on cases. However, you can't assign permissions to any user you choose. Like the features that it enables, each permission has a requirement of its own. To assign a given permission to a user, that user's license (or licenses) must support the permission. A single permission can be supported by more than one license.

Think of permissions as locks, and think of licenses as rings of keys. Before you can assign users a specific permission, they must have a license that includes the key to unlock that permission.

Although every user must have exactly one user license, you can assign one or more permission set licenses or feature licenses to incrementally unlock more permissions.

Continuing our example, the Salesforce user license includes the key to unlock the "Read" permission on cases, but the Force.com—App Subscription user license doesn't. If you try to assign that permission to a Force.com—App Subscription user, you get an error message. However, if that Force.com—App Subscription user is also assigned a Company Community for Force.com permission set license, you can assign "Read" on cases to that user.

Salesforce provides the following types of licenses and usage-based entitlements.

IN THIS SECTION:

User Licenses

A user license determines the baseline of features that the user can access. Every user must have exactly one user license. You assign user permissions for data access through a profile and optionally one or more permission sets.

Permission Set Licenses

A permission set is a convenient way to assign users specific settings and permissions to use various tools and functions. Permission set licenses incrementally entitle users to access features that are not included in their user licenses. Users can be assigned any number of permission set licenses.

Feature Licenses Overview

A feature license entitles a user to access an additional feature that is not included with his or her user license, such as Marketing or Work.com. Users can be assigned any number of feature licenses.

Usage-based Entitlements

A usage-based entitlement is a limited resource that your organization can use on a periodic basis—such as the allowed number of monthly logins to a Partner Community or the record limit for Data.com list users.

User Licenses

A user license determines the baseline of features that the user can access. Every user must have exactly one user license. You assign user permissions for data access through a profile and optionally one or more permission sets.

Example:

- Assign a Force.com user license to Employee A. The Force.com user license only supports standard object permissions for accounts and contacts, so Employee A can't access cases.
- Assign a Salesforce user license to Employee B. Give "Read" access on cases to Employee B.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Edition requirements vary for each user license type.

Salesforce offers these license types.

- Standard User Licenses
- Chatter User Licenses
- Communities User Licenses
- Service Cloud Portal User Licenses
- Sites and Site.com User Licenses
- Authenticated Website User Licenses

Note: If your company has purchased custom user licenses for other types of functionality, you can see other license types listed. Your Salesforce org can also have other licenses that are supported but no longer available for purchase. Contact Salesforce for more information.

The following license types are available only for orgs that use a Customer Portal or partner portal.

- Customer Portal User Licenses
- Customer Portal—Enterprise Administration User Licenses
- Partner Portal User Licenses

If you don't have a Customer Portal or partner portal but want to share information with your customers or partners, see Communities User Licenses on page 223.

IN THIS SECTION:

View Your Organization's User Licenses

View the user licenses that your company has purchased to know what you have available to assign to your users.

Standard User Licenses

Find information about standard user licenses that you can get for your organization, such as the Salesforce user license and Force.com user license types.

Chatter User Licenses

All standard Salesforce licenses allow free Chatter access for everyone in your organization. Salesforce also offers Chatter-specific licenses: Chatter External, Chatter Free, and Chatter Only (also known as Chatter Plus). The Chatter Only license is available for purchase only by existing Chatter Plus customers. For new customers, the Employee Apps Starter license is a step up from Chatter Only, giving your users access to a more robust set of features.

Communities User Licenses

We have three Communities licenses for external users: Customer Community, Customer Community Plus, and Partner Community. We also have Employee Apps Starter and Employee Apps Plus licenses for Employee Communities.

Database.com User Licenses

Service Cloud Portal User Licenses

Sites and Site.com User Licenses

Sites and Site.com users can have Guest User or Site.com Only user licenses.

Authenticated Website User Licenses

Platform portal users have the Authenticated Website license, which is designed to be used with Force.com Sites. It gives named sites users unlimited logins to your Platform Portal to access customer support information.

Customer Portal User Licenses

Users of a Customer Portal site have the Customer Portal Manager Standard license.

Customer Portal—Enterprise Administration User Licenses

Customer Portal—Enterprise Administration users have the Customer Portal Manager Custom license. This license gives contacts unlimited logins to your Salesforce Customer Portal to manage customer support.

Partner Portal User Licenses

Partner Portal users have the Gold Partner user license. They can only access Salesforce using the partner portal.

SEE ALSO:

View and Manage Users

Set Up Your Company in Salesforce

View Your Organization's User Licenses

View the user licenses that your company has purchased to know what you have available to assign to your users.

1. From Setup, enter `Company Information` in the `Quick Find` box, then select **Company Information**.
2. See the User Licenses related list.

EDITIONS

Available in: Salesforce Classic

Available in: All editions

USER PERMISSIONS

To view user licenses:

- View Setup and Configuration

Standard User Licenses

Find information about standard user licenses that you can get for your organization, such as the Salesforce user license and Force.com user license types.

EDITIONS

Available in: Salesforce Classic

Edition requirements vary for each user license type.

License Type	Description	Available in
`Salesforce`	Designed for users who require full access to standard CRM and Force.com AppExchange apps. Users with this user license are entitled to access any standard or custom app. Each license provides additional storage for Enterprise, Unlimited, and Performance Edition users.	All editions
`Knowledge Only User`	Designed for users who only need access to the Salesforce Knowledge app. This license provides access to custom objects, custom tabs, and the following standard tabs. • Articles • Article Management • Chatter • Files • Home • Profile • Reports	**Enterprise**, **Unlimited**, and **Performance** Editions

License Type	Description	Available in
	• Custom objects • Custom tabs The Knowledge Only User license includes a Knowledge Only profile that grants access to the Articles tab. To view and use the Article Management tab, a user must have the “Manage Articles” permission. Note: To view articles, a user must have the “AllowViewKnowledge” permission on their profile. However, this permission is off for default profiles. To give a user the “AllowViewKnowledge” permission on their profile, activate the permission on a cloned profile and assign the cloned profile to the user.	
`Identity`	Grants users access to Salesforce Identity features.Salesforce Identity connects Salesforce users with external applications and services, while giving administrators control over authentication and authorization for these users. For more information, see the *Salesforce Identity Implementation Guide*.	**Enterprise**, **Unlimited**, **Performance**, and **Developer** Editions Ten free Identity user licenses are included with each new **Developer** Edition organization.
`External Identity`	Provides Identity features for users outside of your organization’s user base (such as non-employees). Store and manage these users, choose how they authenticate (username/password, or Single Sign-On social sign-on through Facebook, Google+, LinkedIn, and others), and allow self-registration.	**Enterprise**, **Unlimited**, **Performance**, and **Developer** Editions Five free External Identity user licenses are included with each new **Developer** Edition organization.
`Work.com Only User`	Designed for users who don’t have a Salesforce license and need access to Work.com. Note: Chatter must be enabled for Work.com features to fully function.	**Professional**, **Enterprise**, **Unlimited**, **Performance**, and **Developer** Editions

Force.com User License Types

License type	Description	Available in
`Salesforce Platform`	Designed for users who need access to custom apps but not to standard CRM functionality. Users with this user license are entitled to use custom apps developed in your organization or installed from Force.com AppExchange. In addition, they are entitled to use core platform functionality such as accounts, contacts, reports, dashboards, documents, and custom tabs. These users are not entitled to some user permissions and standard apps, including report subscriptions, standard tabs and objects	**Enterprise**, **Unlimited**, **Performance**, and **Developer** Editions

License type	Description	Available in
	such as forecasts, leads, campaigns, opportunities, and they cannot subscribe to reports. Users with this license can also use Connect Offline. Note: Users with this license can only view dashboards if the running user also has the same license. Users with a Salesforce Platform user license can access all the custom apps in your organization. Each license provides additional storage for Enterprise, Unlimited, and Performance Edition users. Note: To view articles, a user must have the "AllowViewKnowledge" permission on their profile. However, this permission is off for default profiles. To give a user the "AllowViewKnowledge" permission on their profile, activate the permission on a cloned profile and assign the cloned profile to the user.	
`Force.com - One App`	Note: This license is not available for new customers. Designed for users who need access to one custom app but not to standard CRM functionality. Force.com - One App users are entitled to most of the same rights as Salesforce Platform users, plus they have access to an unlimited number of custom tabs. However, they are limited to one custom app, which is defined as up to 10 custom objects. They are also limited to read-only access of the Accounts and Contacts objects. Push Topic object read permission is not available. Note: Users with this license can only view dashboards if the running user also has the same license. Each license provides an additional 20 MB of data storage and 100 MB of file storage, regardless of the Salesforce edition. Note: To view articles, a user must have the "AllowViewKnowledge" permission on their profile. However, this permission is off for default profiles. To give a user the "AllowViewKnowledge" permission on their profile, activate the permission on a cloned profile and assign the cloned profile to the user.	**Enterprise** and **Unlimited** Editions
`Force.com App Subscription`	Grants users access to a Force.com Light App or Force.com Enterprise App, neither of which include CRM functionality. A Force.com Light App has up to 10 custom objects and 10 custom tabs, has read-only access to accounts and contacts, and supports object-level and field-level security. A Force.com Light App can't use the Bulk API or Streaming API. A Force.com Enterprise App has up to 10 custom objects and 10 custom tabs. In addition to the permissions of a Force.com Light App, a Force.com Enterprise App supports record-level sharing, can use the Bulk API and Streaming API, and has read/write access to accounts and contacts.	**Enterprise**, **Unlimited**, and **Performance** Editions

License type	Description	Available in
	Note: Users with this license can only view dashboards if the running user also has the same license. Each Force.com App Subscription license provides an additional 20 MB of data storage per user for Enterprise Edition and 120 MB of data storage per user for Unlimited and Performance Editions, as well as 2 GB of file storage regardless of the edition. Note: To view articles, a user must have the "AllowViewKnowledge" permission on their profile. However, this permission is off for default profiles. To give a user the "AllowViewKnowledge" permission on their profile, activate the permission on a cloned profile and assign the cloned profile to the user.	
`Company Community User`	This is an internal user license for employee communities. It's designed for users to access custom tabs, Salesforce Files, Chatter (people, groups, feeds), and a Community that includes a Site.com site. Company Community users have read-only access to Salesforce Knowledge articles. They can also: • Access up to 10 custom objects and 10 custom tabs • Use Content, Ideas, Assets, and Identity features • Use activities, tasks, calendar, and events • Have access to accounts, contacts, cases, and documents.	**Enterprise**, **Unlimited**, **Performance**, and **Developer** Editions

SEE ALSO:

User Licenses

Chatter User Licenses

All standard Salesforce licenses allow free Chatter access for everyone in your organization. Salesforce also offers Chatter-specific licenses: Chatter External, Chatter Free, and Chatter Only (also known as Chatter Plus). The Chatter Only license is available for purchase only by existing Chatter Plus customers. For new customers, the Employee Apps Starter license is a step up from Chatter Only, giving your users access to a more robust set of features.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Chatter External and Chatter Free licenses are available in: **Group**, **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Contact Manager**, and **Developer** Editions

Chatter Only (also known as Chatter Plus) licenses are available in: **Professional**, **Enterprise Unlimited**, and **Performance** Editions

Employee Apps Starter licenses are available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** editions

Chatter External

This license is for users who are outside of your company's email domain. These external users, also called customers, can be invited to Chatter groups that allow customers. Customers can access information and interact with users only in the groups they're invited to. They have no access to Chatter objects or data.

Chatter Free

The Chatter Free license is for users who don't have Salesforce licenses but must have access to Chatter. These users can access standard Chatter items such as people, profiles, groups, and files, but they can't access any Salesforce objects or data. Chatter Free users can also be Chatter moderators.

Chatter Free users don't see tabs like other Salesforce users. Chatter Free users access feeds, people, groups, and files using the App Launcher in Lightning Experience. In Salesforce Classic, users access these features from links in the page sidebar.

Salesforce administrators can upgrade a Chatter Free license to a standard Salesforce or Employee Apps Starter license at any time. You can't convert a standard Salesforce, Employee Apps Starter, or Chatter Only license to a Chatter Free license.

Chatter Only (Chatter Plus)

The Chatter Only license is also known as the Chatter Plus license. It's available only to existing Chatter Plus customers. The Chatter Plus license is for users who don't have Salesforce licenses but must have access to Chatter and some additional Salesforce objects. Chatter Plus users can be Chatter moderators and have access to standard Chatter people, profiles, groups, and files pages. They can also

- View Salesforce accounts and contacts
- Use Salesforce CRM Content, Ideas, and Answers
- Access dashboards and reports
- Use and approve workflows
- Use the calendar to create and track activities
- View and modify up to 10 custom objects
- Add records to groups

If you're an existing Chatter Plus customer, you can buy more Chatter Plus licenses, or you can upgrade to Employee Apps Starter.

By default, the tabs for standard Salesforce objects are hidden from Chatter Plus users. Expose these tabs if you want to make them available to Chatter Plus users. For more information on Chatter Plus users, see *Chatter Plus Frequently Asked Questions*

Employee Apps Starter (for Partner and Customer Communities)

The Employee Apps Starter license is for users in communities who must have access to Chatter and a wide variety of Salesforce objects. Employee Apps Starter users can be Chatter moderators and have access to standard Chatter people, profiles, groups, and files pages. They can also interact with

- Accounts
- Assets
- Cases
- Contacts
- Dashboards (read only)
- Documents
- External Objects (Salesforce Connect)
- Events and Calendars
- Ideas
- List Views
- Notes and Attachments
- Reports
- Tasks
- Work Orders
- Work Order Line Items

Besides working with these objects, Employee Apps Starter users have access to these Salesforce features, capabilities, and custom objects

- 20-MB data storage per user license, and 2-GB file storage per user license
- 1000 API calls per day per member for Enterprise Edition orgs and 5000 API calls per day per member for Unlimited Edition orgs
- Direct Messages
- 10 custom objects per license (custom objects in managed packages don't count towards this limit)
- Knowledge (read only)
- Roles and Advanced Sharing
- Salesforce App
- Send Email
- Thanks Badges
- Tokens
- Workflow Approvals

Note: For a detailed look at the benefits associated with an Employee Apps Starter license, see Communities User Licenses.

Chatter License Overview

This table shows the list of features that are available for Chatter External, Chatter Free, Chatter Only, and Employee Apps Starter licenses.

Feature	Chatter External (Access limited to items and people in the groups customers are invited to)	Chatter Free	Chatter Only (a.k.a. Chatter Plus)	Employee Apps Starter
Chatter Desktop client	✓	✓	✓	✓
Use the Salesforce app (Downloadable apps require the "API Enabled" profile permission)	✓ Downloadable app users can't access Groups or People list views.	✓	✓	✓
Feeds	✓	✓	✓	✓
File sharing	✓	✓	✓	✓
Files Connect			✓	✓
Groups	✓	✓	✓	✓
Invitations to join groups	✓ Only customers who are also group managers can invite Chatter users from groups they have access to or people outside Chatter.	✓	✓	✓
Profiles	✓	✓	✓	✓
Topics and hash tags		✓	✓	✓
Private messages	✓	✓	✓	✓ (Direct Messages)
Global search	✓ Search results include only those items that customers have access to via groups.	✓	✓	✓
Custom objects			✓ Up to 10 custom objects	✓
Accounts and contacts			✓ Read only	✓
Calendar and events			✓	✓
Content library			✓	✓

Feature	Chatter External (Access limited to items and people in the groups customers are invited to)	Chatter Free	Chatter Only (a.k.a. Chatter Plus)	Employee Apps Starter
Ideas and answers			✓	✓
Reports and dashboards			✓	✓ (access to dashboards is read-only)
Tasks and activities			✓	✓
Using and approving workflows			✓	✓

Communities User Licenses

We have three Communities licenses for external users: Customer Community, Customer Community Plus, and Partner Community. We also have Employee Apps Starter and Employee Apps Plus licenses for Employee Communities.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Learn About the Licenses

Do I need communities licenses to use communities in my org?

In Enterprise, Performance, and Unlimited orgs, you can create up to 100 communities using the Customer Service (Napili), Customer Account Portal, Salesforce Tabs + Visualforce, or the Aloha templates without buying communities licenses. To create communities using Partner Central, you need to purchase Partner Community licenses.

To start creating your community, first enable Communities in your org. Your newly created community has limited access for guest users without licenses. Purchase Community Cloud licenses to allow members to log in, give access to Salesforce objects, or use more page views, based on your business needs.

Note: If your org has legacy portal licenses, you don't need to purchase communities licenses to use communities.

Are community licenses associated with users or a community?

Communities licenses are associated with users, not a specific community. If needed, you can move users with these licenses between communities. If you have unused licenses, you can assign them to users in any community in your org.

Here's another way to think about it: Your community is like an airplane. Each passenger has a different type of ticket (license), and therefore, different levels of access. They're all together on the same ride, but each person has a slightly different experience based on how much the ticket cost.

In addition to supporting communities licenses, Communities supports all internal and portal licenses, including existing Customer Portal, Authenticated Website, and partner portal licenses.

Do usernames have to be unique across the community or Salesforce?

There are different requirements for username uniqueness depending on the type of license your community is using. Customer and Customer Community Plus licenses require unique usernames within the Salesforce org that a community belongs to. Partner Community licenses and Employee Community licenses require unique usernames across all Salesforce orgs that the user belongs to.

How is a license used in an employee community?

Employee Community licenses are supported by two underlying licenses—the Salesforce Platform user license and the Company Community for Force.com permission set license. To assign an Employee Apps Starter or Employee Apps Plus license to a user, first assign the Salesforce Platform user license. Then assign them the Company Community for Force.com permission set license (you may have to create the permission set before you can assign the license).

When you upgrade from Employee Apps Starter license to Employee Apps Plus license, you get more custom objects, and you don't have to make any changes in Setup.

How do community licenses compare to legacy portal licenses?

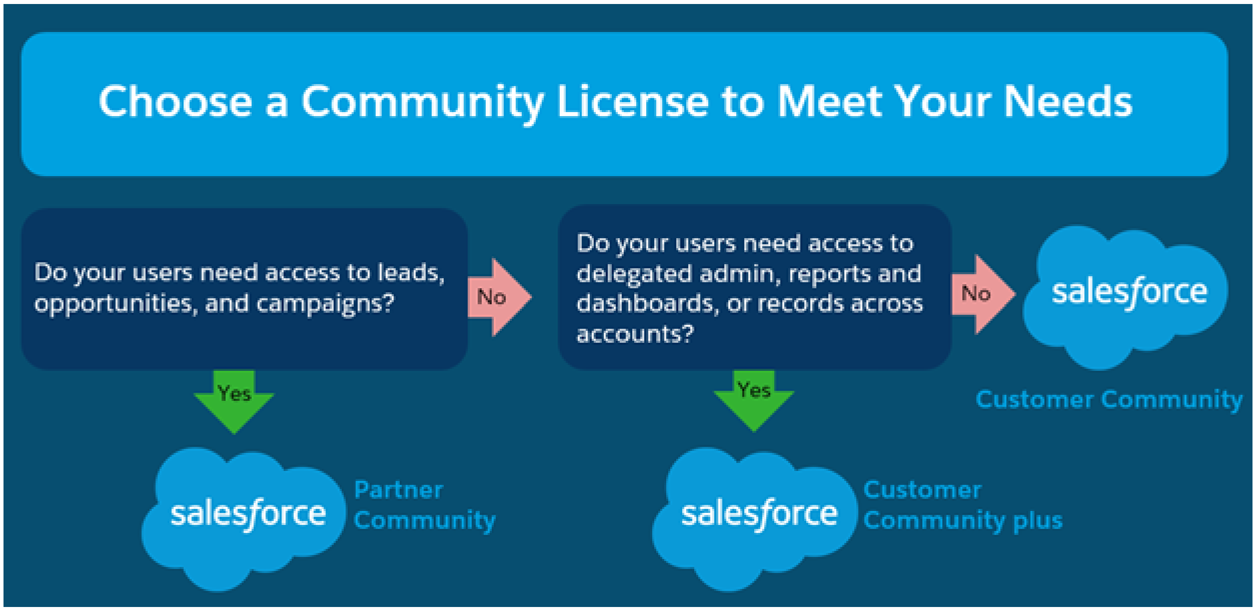
Here's a quick correlation of the new communities licenses with their older portal counterparts and their main use case.

Important: Users who have portal licenses can access your community as long as you include them by adding the profiles or permission sets that they're associated with. You don't have to purchase new Communities licenses for them.

Community License Name	Best Used For	Comparable Portal License
Customer Community	Business-to-consumer communities with large numbers of external users	High Volume Customer Portal, Service Cloud Portal, Authenticated Sites Portal
Customer Community Plus	Business-to-business communities for support and non-sales scenarios, such as eCommerce	Customer Portal — Enterprise Administration
Partner Community	Business-to-business communities that need access to sales data such as partner relationship management	Partner

Here's a simple decision tree to help pick the license type for your community's needs.

Note: Different license types can access your community. Your community is not limited to just one type of license.


Choose a Community License to Meet Your Needs

Do your users need access to leads, opportunities, and campaigns?

Do your users need access to delegated admin, reports and dashboards, or records across accounts?

What about monthly login-based licenses?

The following community licenses are also available as a monthly login-based license, with the following names.

Community License Name	Monthly Login-Based License Name
Customer Community	Customer Community Login License
Customer Community Plus	Customer Community Plus Login License
Partner Community	Partner Community Login License

When using a monthly login-based license, a user consumes a login when signing in to a community. Logged-in users don't consume licenses when switching between their communities. In Winter '18, we introduced an additional metric available in the Company Information section in Setup: Daily Unique Logins. Daily Unique Logins calculates a maximum of one login every 24-hour period per unique user. This calculation doesn't calculate historical data and doesn't include logins that occurred before the metric's installation. Overages are calculated over a 12-month period from the start date of the contract. Entitlements of Logins roll over from month to month and are measured on a 12-month basis from the start of the contract. There's a 1 to 20 login to user ratio limit. For example, if you purchased 1000 monthly logins, you can create up to 20,000 users.

If users with a login-based community license access their communities through the Salesforce app, they consume a login the first time they log in or if their session times out. A login is counted each time a login-based user authenticates to the community. Salesforce calculates logins from the LoginHistory table. Daily Unique Logins through the Salesforce app counts a single login each 24-hour period a user authenticates with Salesforce. The timeout period for a login is configurable up to a maximum of 12 hours.

Is an extra license required to use Community Builder?

Each community using a Community Builder-based template can use the Community Builder to add custom, branded pages to your community. Communities users with the "Create and Set Up Communities" permission automatically have full site administrator access to a community's Community Builder.

Do communities have user limits?

You can have up to 100 communities in your Salesforce org. Active, inactive, and preview communities, including Force.com sites, count against this limit.

To avoid deployment problems and any degradation in service quality, we recommend that the number of users in your community not exceed the limits listed below. If you require additional users beyond these limits, contact your Salesforce account executive. If your growing community needs more users, contact your Salesforce account representative to understand how the product can scale to meet your demands.

Community License Type	Number of Users
Partner or Customer Community Plus	1 million
Customer	10 million

Will unauthenticated users count against my community's licenses?

Not at all! Unauthenticated or guest users who access your community do not use up any of your community's licenses.

Here are the page view limits for guest users, based on your Salesforce edition. Overages are calculated on a yearly basis. If your growing community exceeds this number of guest user page views, contact your Salesforce account representative to increase your page view limits.

Salesforce Edition	Number of Page Views
Enterprise Edition	500,000/month
Unlimited Edition	One million/month

For example, a community set up in an Enterprise Edition org can have up to 6 million page views over the course of a year. Overages will be calculated after the annual limit has been reached. See Community Usage Limits for more information about page view and other user limits.

License Detail

This table shows which features are available to the default user profiles with Customer Community, Customer Community Plus, Partner Community, or Employee Apps licenses.

	Customer Community	Customer Community Plus	Partner Community[1]	Employee Apps Starter	Employee Apps Plus
Salesforce Standard Objects					
Account Contact Relationships (Contacts to Multiple Accounts)[2]	✓	✓	✓	✓	✓
Accounts	✓ Read, Edit[3]	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit, Delete, View All Data, Manage All Data	✓ Read, Create, Edit, Delete, View All Data, Manage All Data
Assets	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit (Can be used for employees, but not for customers)	✓ Read, Create, Edit (Can be used for employees, but not for customers)
Campaigns			✓ Read, Create, and Edit[4]		

[1] **A user with a Partner Community license must be associated with a business account that is enabled as a partner account. Partner users can't be associated with person accounts.**

[2] To view or create relationships between accounts and contacts, you must have "Read" on accounts and contacts. To edit or delete relationships between account and contacts, you must have "Read" on accounts and "Edit" on contacts.

[3] For Customer Community licenses, access can also be controlled using sharing sets.

[4] For the Partner Community license, to read, create, and edit campaigns in the user interface, the partner user also needs the "Marketing User" permission. With these permissions, a partner user can: search for and add their contacts or leads as campaign members, access reports on their campaigns, and mass-email or mass-assign their contacts and leads on a campaign.

	Customer Community	Customer Community Plus	Partner Community[1]	Employee Apps Starter	Employee Apps Plus
Cases	✓ Read, Create, Edit [5]	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit, Delete [6]	✓ Read, Create, Edit, Delete [7]
Contacts	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit, Delete, View All Data, Manage All Data	✓ Read, Create, Edit, Delete, View All Data, Manage All Data
Contracts	✓ Read, Create, Edit, Delete	✓ Read, Create, Edit, Delete	✓ Read, Create, Edit, Delete		
Dashboards		✓ Read Only	✓ Read Only	✓ Read Only	✓ Read Only
Documents	✓ Read Only	✓ Read Only	✓ Read Only	✓ Read, Create, Edit, Delete, View All Data, Manage All Data	✓ Read, Create, Edit, Delete, View All Data, Manage All Data
Entitlements	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit		
External Objects (Salesforce Connect)	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit
Events and Calendar		✓ Read, Create, Edit, Delete	✓ Read, Create, Edit, Delete	✓ Read, Create, Edit, Delete	✓ Read, Create, Edit, Delete
Ideas	✓ Read, Create	✓ Read, Create	✓ Read, Create	✓ Read, Create	✓ Read, Create

[1] **A user with a Partner Community license must be associated with a business account that is enabled as a partner account. Partner users can't be associated with person accounts.**

[5] For the Customer Community license, cases can't be created on behalf of another user.

[6] For Employee Apps Starter licenses, cases can track internal and employee issues, but should not be used for customer cases. Internal employee users must have a Service Cloud license to interact with external cases.

[7] For Employee Apps Plus licenses, cases can track internal and employee issues, but should not be used for customer cases. Internal employee users must have a Service Cloud license to interact with external cases.

	Customer Community	Customer Community Plus	Partner Community[1]	Employee Apps Starter	Employee Apps Plus
Leads			✓ Read, Create, Edit		
List Views	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit
Notes and Attachments	✓ Exceptions apply[8]	✓	✓	✓	✓
Opportunities			✓ Read, Create, Edit		
Orders[9]	✓ Read, Create, Edit, Delete	✓ Read, Create, Edit, Delete	✓ Read, Create, Edit, Delete		
Price Books	✓ Read Only	✓ Read Only	✓ Read Only		
Products	✓ Read Only	✓ Read Only	✓ Read Only		
Quotes			✓ Read, Create, Edit		
Reports[10]		✓ Create and Manage	✓ Create and Manage	✓ Create and Manage	✓ Create and Manage
Service Appointment	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit		
Service Contracts		✓ Read, Create, Edit	✓ Read, Create, Edit		

[1] **A user with a Partner Community license must be associated with a business account that is enabled as a partner account. Partner users can't be associated with person accounts.**

[8] For the Customer Community license, access to Notes and Attachments for most objects is enabled by default. If your users with a Customer Community license can't access Notes and Attachments on accounts and contacts, contact Salesforce.

[9] Once orders are enabled, standard profiles automatically include all object permissions for orders, as well as read access for products and price books. If your external users are assigned to a standard profile and these object permissions aren't appropriate for them, consider creating custom profiles that don't include these object permissions.

[10] To create and edit reports, the user also needs the "Create and Customize Reports," "Report Builder," and "Edit My Reports" permissions. For more information see, Set Up Report Management for External Users—Create and Edit Reports.

	Customer Community	Customer Community Plus	Partner Community[1]	Employee Apps Starter	Employee Apps Plus
Task	✓ Read Only	✓ Read, Create, Edit, Delete	✓ Read, Create, Edit, Delete	✓ Read, Create, Edit, Delete	✓ Read, Create, Edit, Delete
Work Order	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit, Delete (Can be used for employees, but not external users (e.g. customers, partners)	✓ Read, Create, Edit, Delete (Can be used for employees, but not external users (e.g. customers, partners)
Work Order Line Item	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit, Delete	✓ Read, Create, Edit, Delete
Salesforce Features, Capability, and Custom Objects					
Additional Data Storage		2 MB per member (member-based license) 1 MB per member (login-based license)	5 MB per member (member-based license) 1 MB per member (login-based license)	20 MB per user (user-based license)[11]	20 MB per user (user-based license)[12]
API Calls per Day	0	200 per member (member-based license) 10 per member (login-based license)	200 per member (member-based license) 10 per member (login-based license)	1000 per member for Enterprise Edition orgs 5000 per member for Unlimited Edition orgs	1000 per member for Enterprise Edition orgs 5000 per member for Unlimited Edition orgs
Chatter (People, Groups, Feeds, Private Messages)	✓	✓	✓	✓	✓
Custom Objects	✓ 10 custom objects per license (custom	✓ 10 custom objects per license (custom	✓ 10 custom objects per license (custom	✓ 10 custom objects per license (custom	✓ 110 custom objects per license (custom

[1] **A user with a Partner Community license must be associated with a business account that is enabled as a partner account. Partner users can't be associated with person accounts.**

[11] For the Employee Apps Starter license, the data storage limit is 20 MB per user license, and the file storage limit is 2 GB per user license.

[12] For the Employee Apps Plus license, the data storage limit is 20 MB per user license for EE editions, and 120 MB per user license for UE editions. File storage limit is 2 GB per user license.

	Customer Community	Customer Community Plus	Partner Community[1]	Employee Apps Starter	Employee Apps Plus
	objects in managed packages don't count towards this limit, as long as they are made publicly available on AppExchange)	objects in managed packages don't count towards this limit, as long as they are made publicly available on AppExchange))	objects in managed packages don't count towards this limit, as long as they are made publicly available on AppExchange))	objects in managed packages don't count towards this limit, as long as they are made publicly available on AppExchange))	objects in managed packages don't count towards this limit, as long as they are made publicly available on AppExchange))
Delegated Administration		✓	✓		
Files[13] and Content[14]	✓ Content is not available with Customer Community licenses.	✓ Create, Read, Edit, Delete	✓ Create, Read, Edit, Delete	✓ Create, Read, Edit, Delete	✓ Create, Read, Edit, Delete
Knowledge	✓ Read Only	✓ Read Only	✓ Read Only	✓ Read Only	✓ Read Only
Roles and Advanced Sharing		✓	✓	✓	✓
Sharing Sets	✓				
Salesforce App	✓	✓	✓	✓	✓
Send Email		✓	✓[15]	✓	✓
Territory Management			✓		
Thanks Badges[16]	✓	✓	✓	✓	✓
Tokens				✓ Create, Read, Edit, Delete	✓ Create, Read, Edit, Delete

[1] **A user with a Partner Community license must be associated with a business account that is enabled as a partner account. Partner users can't be associated with person accounts.**

[13] Salesforce Files with Chatter enabled lets you share files in a group, feed, and post a file to a record. With Salesforce CRM Content enabled, Files gives you access to Libraries, content deliveries, and file tagging. Salesforce Files Sync is not available in Communities.

[14] Library administrators can manage library permissions to determine the level of access users have to content libraries.

[15] Partner users can't see emails in the case feed.

[16] Thanks features are available in orgs where Chatter is enabled. Thanks badges from internal orgs are not available in Communities, so admins with a Salesforce internal license must create the badges they want to appear. Additional Work.com features, including goals, coaching, and feedback are not available in community orgs.

	Customer Community	Customer Community Plus	Partner Community[1]	Employee Apps Starter	Employee Apps Plus
Workflow Approvals	✓[17]	✓	✓	✓	✓

SEE ALSO:

- User Licenses
- Upgrade Community User Licenses
- Authenticated Website User Licenses
- Partner Portal User Licenses
- Customer Portal User Licenses
- Data and File Storage Limits

Database.com User Licenses

EDITIONS

Available in: Salesforce Classic

Available in: **Database.com** Edition

User License	Description	Default Number of Available Licenses
Database.com Admin	Designed for users who need to administer Database.com, or make changes to Database.com schemas or other metadata using the point-and-click tools in the Database.com Console.	Database.com Edition: 3
Database.com User	Designed for users who need Database.com access to data stored in Database.com.	Database.com Edition: 3 Enterprise, Unlimited, and Database.com Edition: 0 Contact Database.com to obtain Database.com User Licenses

[1] **A user with a Partner Community license must be associated with a business account that is enabled as a partner account. Partner users can't be associated with person accounts.**

[17] Customer Community license holders can submit for approval, but don't have access to approve anything.

User License	Description	Default Number of Available Licenses
Database.com Light User	Designed for users who need only Database.com access to data, need to belong to Database.com groups (but no other groups), and don't need to belong to roles or queues. Access to data is determined by organization-wide sharing defaults.	Database.com Edition: 0 Enterprise, Unlimited, and Database.com Edition: 0 Contact Database.com to obtain Database.com Light User Licenses

SEE ALSO:

User Licenses

Service Cloud Portal User Licenses

EDITIONS

Available in: Salesforce Classic

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

Service Cloud Portal users have the High Volume Customer Portal license. This license gives contacts unlimited logins to your Service Cloud Portal to access customer support information. Users with this license can access accounts, assets, cases, contacts, custom objects, documents, ideas, and questions, depending on their permission settings.

The Overage High Volume Customer Portal license is the same as the High Volume Customer Portal license, except that users do not have unlimited logins. Contact Salesforce for information about the number of Customer Portal licenses you can activate.

This table lists the permissions that can be assigned to Service Cloud portal users.

	Create	Read	Update	Delete
Accounts		✓	✓	
Assets	✓	✓	✓	
Cases	✓	✓	✓	
Contacts	✓	✓	✓	
Custom Objects	✓	✓	✓	✓
Documents		✓		
Ideas	✓	✓		
Knowledge		✓		
Price Books		✓		
Products		✓		
Questions and Answers	✓	✓		

	Create	Read	Update	Delete
Solutions		✓		
Work Orders	✓	✓	✓	

SEE ALSO:

User Licenses

Sites and Site.com User Licenses

Sites and Site.com users can have Guest User or Site.com Only user licenses.

EDITIONS

Available in: Salesforce Classic

Edition requirements vary by user license type.

`Guest User`

Designed for public users who access your Site.com or Force.com sites. If Communities is enabled, these users also have access to public pages in your communities. Site visitors have access to any information made available in an active public site. For each Guest User license, you can develop one site for your organization.

For Site.com, **Developer**, **Enterprise**, **Unlimited**, and **Performance** Editions each come with unlimited Guest User licenses.

For Force.com sites, **Enterprise**, **Unlimited**, and **Performance** Editions come with 25 Guest User licenses. **Developer** Edition comes with one Guest User license.

Note:

- You can't purchase additional Guest User licenses for Force.com sites.
- The Authenticated Website high-volume portal user license is specifically designed to be used with Force.com sites. Because it's designed for high volumes, it should be a cost-effective option to use with Force.com sites.

`Site.com Only`

Designed for **Performance**, **Unlimited**, and **Enterprise** Edition users who need access to Site.com but not to standard CRM functionality. Site.com Only users are entitled to the same rights as Force.com - One App users, plus they have access to the Content app. However, they don't have access to the Accounts and Contacts objects. Users have access to an unlimited number of custom tabs but are limited to the use of one custom app, which is defined as up to 20 custom objects.

Each Site.com Only user also needs either a Site.com Contributor or Site.com Publisher feature license to access Site.com.

SEE ALSO:

User Licenses

Authenticated Website User Licenses

EDITIONS

Available in: Salesforce Classic

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

Platform portal users have the Authenticated Website license, which is designed to be used with Force.com Sites. It gives named sites users unlimited logins to your Platform Portal to access customer support information.

The Overage Authenticated Website license is the same as the Authenticated Website license, except that users do not have unlimited logins.

Note: Once orders are enabled, standard profiles automatically include all object permissions for orders, as well as read access for products and price books. If your external users are assigned to a standard profile and these object permissions aren't appropriate for them, consider creating custom profiles that don't include these object permissions.

This table lists the permissions that can be given to Authenticated Website users.

	Create	Read	Update	Delete
Contracts	✓	✓	✓	✓
Documents		✓		
Ideas	✓	✓		
Knowledge		✓		
Orders	✓	✓	✓	✓
Price Books		✓		
Products		✓		
Custom Objects	✓	✓	✓	✓

SEE ALSO:

User Licenses

Customer Portal User Licenses

EDITIONS

Available in: Salesforce Classic

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

Users of a Customer Portal site have the Customer Portal Manager Standard license.

Note: Starting with Summer '13, these licenses are only available for organizations that already have a Customer Portal. If you don't have a Customer Portal but want to easily share information with your customers, see Communities User Licenses on page 223.

It allows contacts to log in to your Customer Portal to manage customer support. You can associate users who have a Customer Portal Manager Standard license with the Customer Portal User profile or a profile cloned and customized from the Customer Portal User profile. This standard profile lets users view and edit data they directly own or data owned by or shared with users below them in the Customer Portal role hierarchy. These users can also view and edit cases where they are listed in the `Contact Name` field.

Users with the Customer Portal Manager Standard license can:

- View contacts, price books, and products.
- View and edit accounts and cases.

- Create and edit assets.
- Create, view, edit, and delete custom objects.
- Access custom objects depending on their permissions.
- Receive the "Portal Super User" permission.
- Access Salesforce CRM Content if they have a Salesforce CRM Content feature license or the appropriate permissions.

The Overage Customer Portal Manager Standard license is the same as the Customer Portal Manager Standard license, except that users are limited to one login per month.

Note: Once orders are enabled, standard profiles automatically include all object permissions for orders, as well as read access for products and price books. If your external users are assigned to a standard profile and these object permissions aren't appropriate for them, consider creating custom profiles that don't include these object permissions.

This table lists the permissions that can be given to Customer Portal users.

	Create	Read	Update	Delete
Accounts		✓	✓	
Assets	✓	✓	✓	
Cases	✓	✓	✓	
Contacts		✓		
Contracts	✓	✓	✓	✓
Custom Objects	✓	✓	✓	✓
Documents		✓		
Ideas	✓	✓	✓	
Knowledge		✓		
Orders	✓	✓	✓	✓
Price Books		✓		
Products		✓		
Reports and Dashboards [1]	✓	✓	✓	✓
Solutions		✓		
Questions and Answers	✓	✓		

Note:

- [1] To create and edit reports in communities, the user also needs the "Create and Customize Reports," "Report Builder," and "Edit My Reports" permissions. These permissions allow users to create and edit reports in communities, not portals. By default, reports and dashboards are read-only. For more information see, Set Up Report Management for External Users—Create and Edit Reports.

SEE ALSO:

User Licenses

Customer Portal—Enterprise Administration User Licenses

EDITIONS

Available in: Salesforce Classic

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** editions

Customer Portal—Enterprise Administration users have the Customer Portal Manager Custom license. This license gives contacts unlimited logins to your Salesforce Customer Portal to manage customer support.

Note: Starting with Summer '13, these licenses are only available for organizations that already have a Customer Portal. If you don't have a Customer Portal but want to easily share information with your customers, see Communities User Licenses on page 223.

You can associate users who have a Customer Portal Manager Custom license with the Customer Portal User profile or a profile cloned and customized from the Customer Portal User profile, which lets them view and edit data they directly own and view, create, and edit cases where they're listed in the `Contact Name` field.

Users with this license can:

- Create, read, or update accounts, assets, and cases.
- View contacts.
- View custom objects and run reports depending on their permissions.
- Receive the "Portal Super User" and "Delegated External User Administrator" permissions.
- Access Salesforce CRM Content if they have a Salesforce CRM Content feature license or the appropriate permissions.

The Overage Customer Portal Manager Custom license is the same as the Customer Portal Manager Custom license, except that users do not have unlimited logins. Contact Salesforce for information about the number of Customer Portal licenses you can activate.

Note: Once orders are enabled, standard profiles automatically include all object permissions for orders, as well as read access for products and price books. If your external users are assigned to a standard profile and these object permissions aren't appropriate for them, consider creating custom profiles that don't include these object permissions.

This table lists the permissions that can be given to Customer Portal—Enterprise Administration users.

	Create	Read	Update	Delete
Accounts	✓	✓	✓	
Assets	✓	✓	✓	
Cases	✓	✓	✓	
Contacts	✓	✓	✓	
Contracts	✓	✓	✓	✓
Custom Objects	✓	✓	✓	✓
Documents		✓		

	Create	Read	Update	Delete
Ideas	✓	✓	✓	
Knowledge		✓		
Orders	✓	✓	✓	✓
Price Books		✓		
Products		✓		
Reports and Dashboards [1]	✓	✓	✓	✓
Solutions		✓		
Questions and Answers	✓	✓		

Note:

- [1] To create and edit reports in communities, the user also needs the "Create and Customize Reports," "Report Builder," and "Edit My Reports" permissions. These permissions allow users to create and edit reports in communities, not portals. By default, reports and dashboards are read-only. For more information see, Set Up Report Management for External Users—Create and Edit Reports.

SEE ALSO:

User Licenses

Partner Portal User Licenses

Partner Portal users have the Gold Partner user license. They can only access Salesforce using the partner portal.

Note:

- Starting in Summer '13, this license is no longer available for organizations that aren't currently using the partner portal. If you don't have a partner portal but want to easily share information with your partners, see Communities User Licenses on page 223.
- Once orders are enabled, standard profiles automatically include all object permissions for orders, as well as read access for products and price books. If your external users are assigned to a standard profile and these object permissions aren't appropriate for them, consider creating custom profiles that don't include these object permissions.

EDITIONS

Available in: Salesforce Classic

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

This table lists the permissions that can be given to Partner Portal users.

	Create	Read	Update	Delete
Accounts	✓	✓	✓	
Approvals		✓		
Assets	✓	✓	✓	

	Create	Read	Update	Delete
Campaigns[1]	✓	✓	✓	
Cases	✓	✓	✓	
Contacts	✓	✓	✓	
Contracts	✓	✓	✓	✓
Custom Objects	✓	✓	✓	✓
Documents		✓		
Ideas	✓	✓	✓	
Knowledge		✓		
Leads	✓	✓	✓	
Opportunities	✓	✓	✓	
Orders	✓	✓	✓	✓
Price Books		✓		
Products		✓		
Reports and Dashboards[2]	✓	✓	✓	✓
Solutions		✓		
Questions and Answers	✓	✓		

Note:

- [1] A partner portal user can create and edit campaigns in a community but not in a legacy portal. For the Partner Community license, to read, create, and edit campaigns in the user interface, the partner user also needs the "Marketing User" permission. With these permissions, a partner user can: search for and add their contacts or leads as campaign members, access reports on their campaigns, and mass-email or mass-assign their contacts and leads on a campaign.
- [2] To create and edit reports in communities, the user also needs the "Create and Customize Reports," "Report Builder," and "Edit My Reports" permissions. These permissions allow users to create and edit reports in communities, not portals. By default, reports and dashboards are read-only. For more information see, Set Up Report Management for External Users—Create and Edit Reports.

SEE ALSO:

User Licenses

Permission Set Licenses

A permission set is a convenient way to assign users specific settings and permissions to use various tools and functions. Permission set licenses incrementally entitle users to access features that are not included in their user licenses. Users can be assigned any number of permission set licenses.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

The availability of each permission set license depends on the edition requirements for permission sets and the related feature.

IN THIS SECTION:

SEE ALSO:

Set Up Your Company in Salesforce

What Are Permission Set Licenses?

Permission set licenses incrementally entitle users to access features that are not included in their user licenses. Users can be assigned any number of permission set licenses.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

The availability of each permission set license depends on the edition requirements for permission sets and the related feature.

Tip: Permission sets and permission set licenses have different purposes. Read on to save yourself some trouble later.

- **Permission set licenses** extend the functionality of user licenses. With permission set licenses, you can assign more permissions to users than their user license supports.
- **Permission sets** contain settings that grant users permissions. Permission sets extend users’ functional access without changing their profiles.

You can create a permission set for a specific feature’s permission set license. Enable the selected permission set license permissions within the permission set. Then, users assigned to the permission set are granted the functionality in it that you chose.

You can also create a permission set that is not specific to a single user license or permission set license. First, assign users to the permission set licenses you want. Then, assign them to the permission set you created and enable the permissions you need.

Note: Salesforce validates if users have the licenses required for a permission set. If you assign users to a permission set who don’t have the user permissions required, you receive an assignment error.

Check out this table for examples of how different permission set and permission set license combinations affect users. Most features backed by permission set licenses require that you create a permission set for its permissions, but not all do. The Sales Console permission set license comes with a permission set already created for you.

Example Use Case	What You'd Do	Result
Associate a permission that is backed by a single permission set license, such as Identity Connect, with a permission set.	1. Create a permission set. In the license dropdown menu, select **Identity Connect**. 2. Notice that the permission set settings page shows only the settings available with the Identity Connect permission set license. Enable **Use Identity Connect**.	Users assigned to the permission set are granted the Identity Connect permission.
Associate permissions that are backed by more than one permission set license with a permission set. For example, you could associate the following permission set licenses with a single permission set you create: - Identity Connect - Dialer Inbound User - Dialer Outbound User	1. Assign the Identity Connect, Dialer Inbound User, and Dialer Outbound User permission set licenses to the users who need them. 2. Create a permission set. In the license dropdown menu, select **--None--**. 3. In your permission set, enable the following permissions: - **Use Identity Connect** - **Access Dialer Inbound Calls** - **Access Dialer Outbound Calls**	Users assigned to the permission set are granted the Identity Connect, Dialer Inbound Calls, and Dialer Outbound Calls permissions.
Associate a permission that is backed by a permission set license and also include other user permissions. For example, you could create a permission set with the permissions backed by the Identity Connect permission set license and also include the Lightning Experience User permission.	1. Assign the Identity Connect permission set license to the users who need it. 2. Create a permission set. In the license dropdown menu, select **--None--**. 3. In your permission set, enable the following permissions: - **Use Identity Connect** - **Lightning Experience User**	Users assigned to the permission set are granted the Identity Connect and Lightning Experience User permissions.

SEE ALSO:

Permission Set Licenses

User Licenses

Create Permission Sets

App and System Settings in Permission Sets

Assign a Feature Permission Set License and Permission Set

Make sure to follow instructions for your permission set license-related feature. You can't add permission sets that are associated with permission set licenses to managed packages.

Note: If you purchased a license that comes with standard permission sets, such as Sales Console User, permission sets are auto-generated for you.

1. From Setup, enter `Company Information` in the `Quick Find` box, then select **Company Information** and scroll down to Permission Set Licenses.
   You can see how many permission set licenses are available and have already been assigned. You can also see how many types of permission set licenses you have for different features.
2. From Setup, enter `Permission Sets` in the `Quick Find` box, then select **Permission Sets**.
3. Click **New**.
4. Enter your permission set information.
5. For License, select the license to associate with this permission set.

EDITIONS

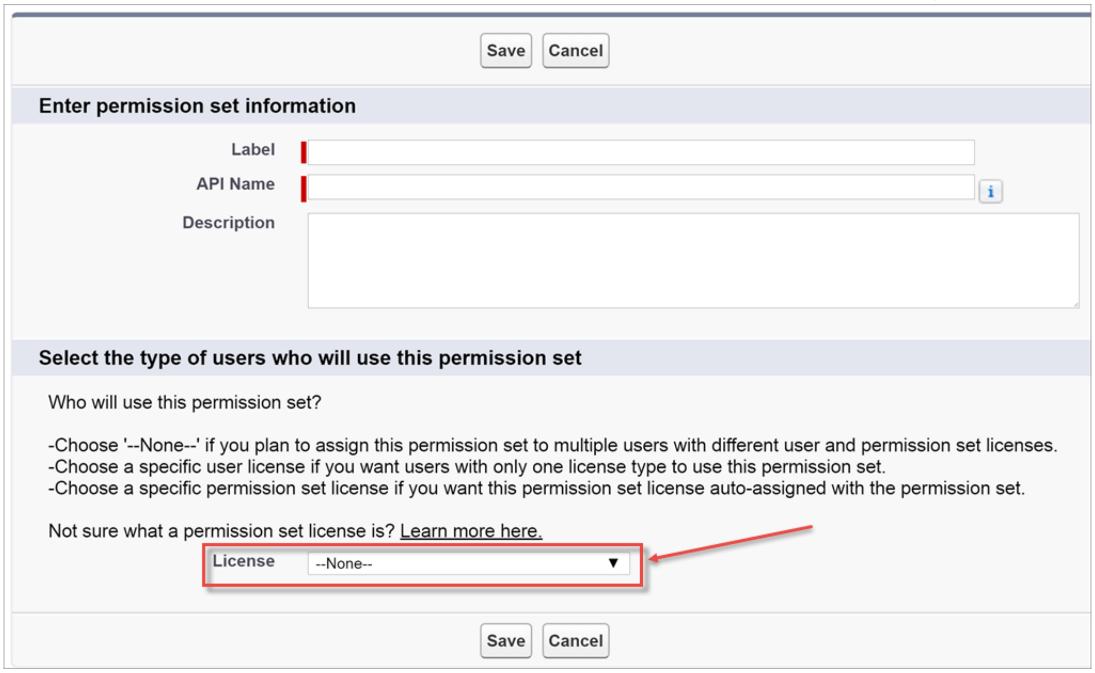
Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To assign a permission set license:
- Manage Users

To assign a permission set to users:
- Assign Permission Sets



Enter permission set information

Label

API Name

Description

Select the type of users who will use this permission set

Who will use this permission set?

-Choose '--None--' if you plan to assign this permission set to multiple users with different user and permission set licenses.
-Choose a specific user license if you want users with only one license type to use this permission set.
-Choose a specific permission set license if you want this permission set license auto-assigned with the permission set.

Not sure what a permission set license is? Learn more here.

License --None--

When you select a specific permission set license, any user assigned to the permission set is *auto-assigned* the permission set license. If you select --None--, you must *manually* assign the permission set license to users before you can add them to the new permission set.

6. Select the feature permissions to enable for your permission set. Use `Find Settings` to search for them quickly. Refer to the documentation for your feature to see which permissions are available with a specific permission set license.

Example: Let's say you purchased an Identity Connect permission set license. This permission set license contains a permission that grants access to the Identity Connect product features, such as providing Active Directory integration. To grant a user access to this permission:

- Ensure that the user has the Identity Connect permission set license. Users who don't have the associated permission set license for a permission set you create can't use the permission set. You can check which permission set licenses a user has by viewing the Permission Set License Assignments section of the user detail page.
- Create a permission set and name it something like "Identity Connect Permissions." From License, choose **Identity Connect**. While still in the permission set, go to `Find Settings`, search for **Identity Connect**, and select the **Use Identity Connect** system permission.
- Assign a user to the permission set.

View Your Salesforce Org's Permission Set Licenses

View the permission set licenses your organization has purchased to know what you have available to assign to your users.

1. From Setup, enter *Company Information* in the `Quick Find` box, then select **Company Information**.
2. View the Permission Set Licenses related list.

For information on purchasing permission set licenses, contact Salesforce.

SEE ALSO:

Permission Set Licenses

Assign a Permission Set License to a User

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view permission set licenses:

- View Setup and Configuration

Assign a Permission Set License to a User

You might need to assign a permission set license to a user before you can assign some permissions.

Tip: Before beginning, check if the permission set license is already associated with a permission set. If so, save yourself time and simply assign the user to that permission set. If not, you might need to assign the permission set license to users to grant them access to the permission set license functionality.

1. From Setup, enter *Users* in the `Quick Find` box, then select **Users**.
2. Click the name of the user to whom you want to assign the permission set license.
3. In the Permission Set License Assignments related list, click **Edit Assignments**.
4. Select the permission set license to assign.

Add the related permission to a permission set and then assign that permission set to the user.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To assign a permission set license:

- Manage Users

Note: After assigning the CRM User, Sales User, or Service User permission set license, assigning a permission set isn't required.

SEE ALSO:

Permission Set Licenses

Remove a Permission Set License from a User

Permission Sets

Assign Permission Sets to a Single User

Remove a Permission Set License from a User

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To remove a permission set license:

- Manage Users

First remove or modify the relevant assigned permission sets that require the license, and then remove the assigned permission set license.

1. Identify the permission that requires the permission set license you want to remove.
2. Make sure that permission isn't assigned to the user through a permission set. You can do that in one of these ways.
   - Remove the permission from the permission sets assigned to the user
   - Remove the permission set from the user's assigned permission sets
3. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.
4. Click the name of the user whose permission set license you want to remove.
5. In the Permission Set License Assignments related list, click **Del** next to the permission set license that you want to remove, and then click **OK**.

SEE ALSO:

Permission Set Licenses

View Your Salesforce Org's Permission Set Licenses

Assign a Permission Set License to a User

Feature Licenses Overview

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Edition requirements vary for each feature licenses.

A feature license entitles a user to access an additional feature that is not included with his or her user license, such as Marketing or Work.com. Users can be assigned any number of feature licenses.

- View the feature licenses enabled for your organization
- Enable users to use a feature
- See all feature licenses currently available in Salesforce

Depending on the features that are enabled for your organization, you might be able to assign more than one type of feature license to your users.

IN THIS SECTION:

View Your Organization's Feature Licenses

View the feature licenses your company has purchased to know what you have available to assign to your users.

Enable a Feature License for a User

You can enable a feature for a user in your organization when creating or editing that user.

Available Feature Licenses

Assign one or more of these additional feature licenses to users so that they can access features not included in their user license.

SEE ALSO:

View and Manage Users

Set Up Your Company in Salesforce

View Your Organization's Feature Licenses

View the feature licenses your company has purchased to know what you have available to assign to your users.

1. From Setup, enter `Company Information` in the `Quick Find` box, then select **Company Information**.
2. See the Feature Licenses related list.

For information on purchasing feature licenses, contact Salesforce.

SEE ALSO:

Feature Licenses Overview

Available Feature Licenses

Enable a Feature License for a User

View and Manage Users

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view feature licenses:

- View Setup and Configuration

Enable a Feature License for a User

You can enable a feature for a user in your organization when creating or editing that user.

1. In Setup, enter `Users` in the `Quick Find` box, then select **Users**.
2. In the user list view, click a user's name.
3. On the User Detail page, select the checkbox next to the feature license you want to enable for that user.

   You can enable more than one feature license for a single user.
4. Click **Save**.

SEE ALSO:

Edit Users

Add a Single User

Feature Licenses Overview

Available Feature Licenses

View Your Organization's Feature Licenses

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To enable feature licenses:

- Manage Internal Users

Available Feature Licenses

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Assign one or more of these additional feature licenses to users so that they can access features not included in their user license.

Feature License	Enables a User to
`Chatter Answers User`	Access Chatter Answers. This feature license is automatically assigned to high-volume portal users who self-register for Chatter Answers.
`Force.com Flow User`	Run flows.
`Knowledge User`	Access Salesforce Knowledge.
`Live Agent User`	Access to Live Agent.
`Marketing User`	Create, edit, and delete campaigns, configure advanced campaign setup, and add campaign members and update their statuses with the Data Import Wizard.
`Mobile User`	Access Salesforce Mobile Classic.
`Offline User`	Access Connect Offline.
`Salesforce CRM Content User`	Access Salesforce CRM Content.
`Service Cloud User`	Access the Salesforce Console for Service. Note: Access to the Salesforce Console for Sales requires the `Sales Console User` permission set license.
`Site.com Contributor User`	Edit site content on Site.com Studio.
`Site.com Publisher User`	Create and style websites, control the layout and functionality of pages and page elements, and add and edit content on Site.com Studio.
`Work.com User`	Access to Work.com objects and permissions.

SEE ALSO:

- View Your Organization's Feature Licenses
- Enable a Feature License for a User
- View and Manage Users
- Feature Licenses Overview

Usage-based Entitlements

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

A usage-based entitlement is a limited resource that your organization can use on a periodic basis—such as the allowed number of monthly logins to a Partner Community or the record limit for Data.com list users.

Some entitlements are persistent. These entitlements give your Salesforce org a set number of the resource, and the amount allowed doesn't change unless your contract is changed. For example, if your company purchases monthly subscriptions for 50 members to access a Partner Community, you can assign up to 50 individuals the ability to log into the community as many times as they want.

Other entitlements are not persistent; these work like credit. Your org can use up to the amount allowed of that entitlement over the time indicated by the resource's frequency. If the entitlement has a frequency of Once, your org will have to purchase more of the resource to replenish the allowance. If the entitlement has a frequency of Monthly, the start and end of the month is determined by your contract, rather than the calendar month.

For example:

- Company A purchases 50 monthly logins for a Partner Community, and on January 15 that org has a pool of 50 logins. Each time someone logs in, one login is used. On February 15, no matter how many were used in the previous month, the pool is refreshed and 50 logins are available through March 14.
- Company B purchases 2,000 records for Data.com list users with an end date of May 15. That org's list users can add or export up to 2,000 records until that date. If the org reaches that limit before May 15, the Data.com list users won't be able to add or export additional records. To unblock users, Company B can purchase additional allowance for that resource.

Note: If your org has multiple contracts with the same `Resource` and the `Resource ID` is `(tenant)`, you will still only see one row for that entitlement, but the data in that row will reflect your combined contracts. In this case, `Start Date` reflects the earliest start date among those contracts, and `End Date` reflects the latest end date among those contracts.

Like feature licenses, usage-based entitlements don't limit what you can do in Salesforce; they add to your functionality. If your usage exceeds the allowance, Salesforce will contact you to discuss additions to your contract.

IN THIS SECTION:

View Your Salesforce Org's Usage-Based Entitlements

Look at your company's usage-based entitlements to know which resources your org is entitled to.

Usage-based Entitlement Fields

The Usage-based Entitlements related list displays the following information. These fields aren't editable, and they are only visible if your Salesforce org is entitled to a resource.

SEE ALSO:

Set Up Your Company in Salesforce

View and Manage Users

View Your Salesforce Org's Usage-Based Entitlements

Look at your company's usage-based entitlements to know which resources your org is entitled to.

1. From Setup, enter *`Company Information`* in the `Quick Find` box, then select **Company Information**.
2. At the bottom of the Company Information page, view the Usage-Based Entitlements related list.

SEE ALSO:

Usage-based Entitlements

Usage-based Entitlement Fields

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view usage-based entitlements:

- View Setup and Configuration

Usage-based Entitlement Fields

The Usage-based Entitlements related list displays the following information. These fields aren't editable, and they are only visible if your Salesforce org is entitled to a resource.

Column name	Description
`Resource`	What your company can use.
`Resource ID`	Unique identifier for this line item.
`Start Date`	Day your contract begins. Note: If you have multiple contracts affecting this resource, this field reflects the earliest start date among your contracts.
`End Date`	Day your contract ends. Note: If you have multiple contracts affecting this resource, this field reflects the latest end date among your contracts.
`Frequency`	If Monthly, `Allowance` is reset at the beginning of each month. If Once, `Allowance` is available until `End Date`.
`Allowance`	Amount of a resource that your org can use. If `Frequency` is Monthly, the month begins on your `Start Date`.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Column name	Description
`Amount Used`	The amount of this resource that your org is using.
`Last Updated`	The most recent date and time when Salesforce took a snapshot of your org's usage for this resource.

For more information about resources your org is entitled to, contact Salesforce.

SEE ALSO:

Usage-based Entitlements

View Your Salesforce Org's Usage-Based Entitlements

Passwords

Salesforce provides each user in your organization with a unique username and password that must be entered each time a user logs in. As an administrator, you can configure several settings to ensure that your users' passwords are strong and secure.

- Password policies—Set various password and login policies, such as specifying an amount of time before all users' passwords expire and the level of complexity required for passwords. See Set Password Policies on page 581.
- User password expiration—Expire the passwords for all users in your organization, except for users with "Password Never Expires" permission. See Expire Passwords for All Users on page 584.
- User password resets—Reset the password for specified users. See Reset Passwords for Your Users on page 252.
- Login attempts and lockout periods—If a user is locked out of Salesforce because of too many failed login attempts, you can unlock them. See Edit Users on page 197.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Password policies available in: **All** Editions

USER PERMISSIONS

To set password policies:

- Manage Password Policies

To reset user passwords and unlock users:

- Reset User Passwords and Unlock Users

Password Requirements

A password can't contain a user's username and can't match a user's first or last name. Passwords also can't be too simple. For example, a user can't change their password to `password`.

For all editions, a new organization has the following default password requirements. You can change these password policies in all editions, except for Personal Edition.

- A password must contain at least eight characters, including one alphabetic character and one number.
- The security question's answer can't contain the user's password.
- When users change their password, they can't reuse their last three passwords.

IN THIS SECTION:

Set Password Policies

Improve your Salesforce org security with password protection. You can set password history, length, and complexity requirements along with other values. In addition, you can specify what to do if a user forgets their password.

Reset Passwords for Your Users

As an administrator, you can reset a user's password for better protection or to unlock a user if the user is locked out.

Expire Passwords for All Users

As an administrator, you can expire passwords for all users any time you want to enforce extra security for your organization. After expiring passwords, all users are prompted to reset their password the next time they log in.

SEE ALSO:

Change Your Password

Set Password Policies

Improve your Salesforce org security with password protection. You can set password history, length, and complexity requirements along with other values. In addition, you can specify what to do if a user forgets their password.

For your organization's security, you can set various password and login policies.

Note: User passwords cannot exceed 16,000 bytes.

Logins are limited to 3,600 per hour per user. This limit applies to organizations created after Summer '08.

1. From Setup, enter `Password Policies` in the `Quick Find` box, then select **Password Policies**.
2. Customize the password settings.

Field	Description
`User passwords expire in`	The length of time until user passwords expire and must be changed. The default is 90 days. This setting isn't available for Self-Service portals. This setting doesn't apply to users with the "Password Never Expires" permission. If you change the `User passwords expire in` setting, the change affects a user's password expiration date if that user's new expiration date is earlier than the old expiration date or if you remove an expiration by selecting `Never expires`.
`Enforce password history`	Save users' previous passwords so that they must always reset their password to a new, unique password. Password history is not saved until you set this value. The default is `3 passwords remembered`. You cannot select `No passwords remembered` unless you select `Never expires` for the `User passwords expire in` field.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To set password policies:
- Manage Password Policies

Field	Description
	This setting isn't available for Self-Service portals.
`Minimum password length`	The minimum number of characters required for a password. When you set this value, existing users aren't affected until the next time they change their passwords. The default is `8 characters`.
`Password complexity requirement`	The requirement for which types of characters must be used in a user's password. Complexity levels: • `No restriction`—allows any password value and is the least secure option. • `Must mix alpha and numeric characters`—requires at least one alphabetic character and one number, which is the default. • `Must mix alpha, numeric, and special characters`—requires at least one alphabetic character, one number, and one of the following special characters: `! # $ % - _ = + < >`. • `Must mix numbers and uppercase and lowercase letters`—requires at least one number, one uppercase letter, and one lowercase letter. • `Must mix numbers, uppercase and lowercase letters, and special characters`—requires at least one number, one uppercase letter, and one lowercase letter, and one of the following special characters: `! # $ % - _ = + < >`. Note: Only the special characters listed meet the requirement. Other symbol characters are not considered special characters.
`Password question requirement`	The values are `Cannot contain password`, meaning that the answer to the password hint question cannot contain the password itself; or `None`, the default, for no restrictions on the answer. The user's answer to the password hint question is required. This setting is not available for Self-Service portals, Customer Portals, or partner portals.
`Maximum invalid login attempts`	The number of login failures allowed for a user before they become locked out. This setting isn't available for Self-Service portals.
`Lockout effective period`	The duration of the login lockout. The default is 15 minutes. This setting isn't available for Self-Service portals. Note: If users are locked out, they must wait until the lockout period expires. Alternatively, a user with the "Reset

Field	Description
	User Passwords and Unlock Users" permission can unlock them from Setup with the following procedure: **a.** Enter *Users* in the Quick Find box. **b.** Select **Users**. **c.** Selecting the user. **d.** Click **Unlock**. This button is only available when a user is locked out.
Obscure secret answer for password resets	This feature hides answers to security questions as you type. The default is to show the answer in plain text. Note: If your org uses the Microsoft Input Method Editor (IME) with the input mode set to Hiragana, when you type ASCII characters, they're converted in Japanese characters in normal text fields. However, the IME doesn't work properly in fields with obscured text. If your org's users cannot properly enter their passwords or other values after enabling this feature, disable the feature.
Require a minimum 1 day password lifetime	When you select this option, a password can't be changed more than once in a 24-hour period.

3. Customize the forgotten password and locked account assistance information.

   Note: This setting is not available for Self-Service portals, Customer Portals, or partner portals.

Field	Description
Message	If set, this message appears in the "We can't reset your password" email. Users receive this email when they lock themselves out by trying to reset their password too many times. The text also appears at the bottom of the Answer Your Security Question page when users reset their passwords. You can tailor the text to your organization by adding the name of your internal help desk or a system administrator. For the email, the message appears only for accounts that need an administrator to reset them. Lockouts due to time restrictions get a different system email message.
Help link	If set, this link displays with the text defined in the Message field. In the "We can't reset your password" email, the URL displays exactly as typed in the Help link field, so the user can see

Field	Description
	where the link goes. This URL display format is a security feature, because the user is not within a Salesforce organization. On the Answer Your Security Question page, the `Help link` URL combines with the text in the `Message` field to make a clickable link. Security isn't an issue, because the user is in a Salesforce organization when changing passwords. Valid protocols: • http • https • mailto

4. Specify an alternative home page for users with the "API Only User" permission. After completing user management tasks such as resetting a password, API-only users are redirected to the URL specified here, rather than to the login page.
5. Click **Save**.

SEE ALSO:

View and Edit Password Policies in Profiles

Passwords

Reset Passwords for Your Users

As an administrator, you can reset a user's password for better protection or to unlock a user if the user is locked out.

To reset a user's password:

1. From Setup, enter *`Users`* in the `Quick Find` box, then select **Users**.
2. Select the checkbox next to the user's name. Optionally, to change the passwords for all currently displayed users, check the box in the column header to select all rows.
3. Click **Reset Password**. The user receives an email that contains a link and instructions to reset the password.

A password created this way doesn't expire, but users must change the password the first time they log in.

Tip: You can perform this and other administration tasks from the SalesforceA mobile app.

Considerations for Resetting Passwords

- Only an administrator can reset single sign-on user passwords. Single sign-on users can't reset their own passwords.
- After resetting a password, users might be required to activate their computers to successfully log in to Salesforce.
- Resetting a locked-out user's password automatically unlocks the user's account.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To reset passwords:

- Reset User Passwords and Unlock Users

  OR

  Permission to edit the user via the user interface or the API

- When a user loses a password, the user can click the forgot password link on the login page to receive an email with steps to reset a password. The user must correctly answer the security question to reset the password. In Password Policies, you can customize the security question page that the user sees with information about where to go to for help.

  Note: If the user hasn't set a security question, or doesn't answer the security question correctly, the password isn't reset.

  A user can request to reset a password through the forgot password link a maximum of five times in a 24-hour period. Administrators can reset a user's password as often as needed.

- Resetting a password also resets the user's security token.

SEE ALSO:

Reset Your Forgotten Password

Change Your Password

Reset Your Security Token

Passwords

Help Users From Anywhere With SalesforceA

Expire Passwords for All Users

As an administrator, you can expire passwords for all users any time you want to enforce extra security for your organization. After expiring passwords, all users are prompted to reset their password the next time they log in.

To expire passwords for all users, except those users with the "Password Never Expires" permission:

1. From Setup, enter *`Expire All Passwords`* in the `Quick Find` box, then select **Expire All Passwords**.
2. Select **Expire all user passwords**.
3. Click **Save**.

The next time users log in, they are prompted to reset their password.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To expire all passwords:

- Reset User Passwords and Unlock Users

Considerations When Expiring Passwords

- Users might need to activate their computers to log in to Salesforce.
- `Expire all user passwords` doesn't affect Self-Service portal users, because they aren't direct Salesforce users.

SEE ALSO:

Passwords

Control Login Access

Control whether your users are prompted to grant account access to Salesforce admins, and whether users can grant access to publishers.

1. From Setup, enter `Login Access Policies` in the `Quick Find` box, then select **Login Access Policies**.
2. To allow Salesforce admins to log in as any user in the org without first asking them to grant access, enable **Administrators Can Log in as Any User**.

   To have this feature removed from your org, contact Salesforce. If you remove the feature, a user must grant login access before a Salesforce admin can log in to that user's account for troubleshooting.
3. To prevent users from granting access to a publisher—for example, to comply with regulatory or privacy concerns—click **Available to Administrators Only** for that publisher.

   Note: Users can't grant login access to managed packages that are licensed to your entire Salesforce org. Only admins with the "Manage Users" permission enabled on their profiles can grant access to these publishers. Also, some managed packages don't have login access. If a package isn't listed on the Login Access Policies page, login access isn't available for that package.
4. Click **Save**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experienc

Available in: **All** Editions

Granting administrator access available in: **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

USER PERMISSIONS

To control login access policies:
- Manage Login Access Policies

SEE ALSO:

Log In as Another User

Grant Login Access

Log In as Another User

To assist other users, administrators can log in to Salesforce as another user. Depending on your organization settings, individual users might need to grant login access to administrators.

Note:

- As a security measure, when administrators are logged in as another user, they can't authorize OAuth data access for that user. For example, admins can't authorize OAuth access to user accounts, including single sign-on to third-party applications.
- If admins attempt to log in as another user who has the "Two-Factor Authentication for User Interface Logins" user permission, they must satisfy the two-factor authentication requirement. Coordinate with the users whom you're logging in as so that they're available when you need account access. They must verify their identity with an authenticator app, U2F security key, or a temporary identity verification code. If a user hasn't already set up a two-factor authentication method, setup is required before you can log in as the user.

1. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.
2. Click the **Login** link next to the username. This link is available only for users who have granted login access to an administrator or in organizations where administrators can log in as any user.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To log in as another user:
- Modify All Data

3. To return to your administrator account, click `User’s Name` > **Logout**.

SEE ALSO:

- Control Login Access
- Grant Login Access
- Troubleshoot Login Issues
- View and Manage Users

Delegate Administrative Duties

Use delegated administration to assign limited admin privileges to users in your org who aren’t administrators. For example, let’s say you want the Customer Support team manager to manage users in the Support Manager role and all subordinate roles. Create a delegated admin for this purpose so that you can focus on other administration tasks.

Delegated administrators can:

- Create and edit users in specified roles and all subordinate roles. User editing tasks include resetting passwords, setting quotas, creating default opportunity teams, and creating personal groups for those users.
- Unlock users.
- Assign users to specified profiles.
- Assign or remove permission sets for users in their delegated groups.
- Create public groups and manage membership in specified public groups.
- Log in as a user who has granted login access to the administrator.
- Manage custom objects and customize nearly every aspect of a custom object. However, a delegated admin can’t create or modify relationships on the object or set org-wide sharing defaults.
- Administer users across all delegated groups to which the delegated admin is assigned. For example, Sam Smith is specified as a delegated administrator in two delegated groups, Group A and Group B. Sam can assign a permission set or public group from Group A to users in Group B.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To manage delegated administration:
- Customize Application

To be a delegated administrator:
- View Setup and Configuration

Note: When delegating administration, keep the following in mind. Delegated administrators:

- Can’t assign profiles or permission sets with the “Modify All Data” permission
- Don’t see the None Specified option when selecting a role for new users
- Need access to custom objects to access the merge fields on those objects from formulas
- Can’t modify permission sets

To delegate administration of particular objects, use object permissions, such as “View All” and “Modify All,” instead.

IN THIS SECTION:

Define Delegate Administrators

Enable delegated administrators to manage users in specified roles and all subordinate roles. You can assign specified profiles to those users, and log in as users who have granted login access to administrators. A delegated administration group is a group of users who have the same admin privileges. These groups are not related to public groups used for sharing.

Define Delegate Administrators

Enable delegated administrators to manage users in specified roles and all subordinate roles. You can assign specified profiles to those users, and log in as users who have granted login access to administrators. A delegated administration group is a group of users who have the same admin privileges. These groups are not related to public groups used for sharing.

1. From Setup, enter `Delegated Administration` in the `Quick Find` box, then select **Delegated Administration** and click **New**
2. Select or create a delegated group.
3. To allow the users in this group to log in as users in the role hierarchy that they administer, select **Enable Group for Login Access**. Depending on your org settings, individual users need to grant login access to allow their administrators to log in as them.
4. Click **Save**.
5. For each related list, click **Add** to define your delegated group details.

SEE ALSO:

Delegate Administrative Duties

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To manage delegated administration:
- Customize Application

To be a delegated administrator:
- View Setup and Configuration

Topics and Tags Settings

When you enable topics for objects, users can add topics to records so they can quickly retrieve related items using list views. With Chatter enabled, users can also see related items on the Records tab of each topic detail page. Enabling topics for an object disables public tags on records of that object type. Personal tags aren't affected.

To use topics to organize records, enable topics for accounts, assets, campaigns, cases, contacts, contracts, files, leads, opportunities, orders, solutions, custom objects, and English articles.

IN THIS SECTION:

Enable and Configure Topics for Objects

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

Enable Tags

Allow users to add personal or public tags to most records. Tags are words or short phrases that users associate to records to describe and organize data in a personalized way.

Adding Tags to the Sidebar

Delete Personal Tags for Deactivated Users

Your org can have up to 5,000,000 personal and public tags applied to records across all users. If your org is approaching this limit, delete personal tags for deactivated users.

EDITIONS

Available in: Salesforce Classic

Topic and tag settings are available in: **All** Editions

USER PERMISSIONS

To modify topic and tag settings:
- Customize Application

Enable and Configure Topics for Objects

Enable topics for objects so 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: **Essentials**,**Group**, **Enterprise**, **Professional**, **Performance**, **Unlimited**, **Contact Manager**, and **Developer** Editions

USER PERMISSIONS

To enable topics for objects:
- Customize Application

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 only supported on 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.)
5. Click **Save** to save changes for all objects.

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

Additionally, if your organization uses Chatter, users can click any topic assigned to a record to go directly to a topic page. There, they'll find other records on the topic, people who are knowledgeable about the topic, and other related information.

SEE ALSO:

Organize Records with Tags and Topics

Add Topics to Records

Enable Tags

EDITIONS

Available in: Salesforce Classic

Tag settings available in: **All** Editions

USER PERMISSIONS

To modify tag settings:
- Customize Application

Allow users to add personal or public tags to most records. Tags are words or short phrases that users associate to records to describe and organize data in a personalized way.

1. From Setup, enter *Tag Settings* in the `Quick Find` box, then select **Tag Settings**.
2. Select **Enable Personal Tags** and **Enable Public Tags** to allow users to add personal and public tags to records. Deselect both options to disable tags.
3. Specify which objects and page layouts display tags in a tag section at the top of record detail pages. The tag section is the only place where a user can add tags to a record.

   For example, if you select only account page layouts, users in your org can only tag account records. If you select only account page layouts for personal tags and not public tags, users can tag account records only with personal tags.
4. Click **Save**.

When enabling tags, keep these guidelines in mind.

- You can also add tags to page layouts by editing a layout directly. However, you can’t add tags to feed-based page layouts.
- Search results and the Tags page don’t display custom objects without an associated tab, even if tags are enabled for the custom object. If you want custom object records to appear, create an associated tab. The tab doesn’t have to be visible to users.
- Customer Portal users can't view the tags section of a page, even if it is included in a page layout.
- When Chatter is disabled, joined reports can’t be tagged.

SEE ALSO:

Topics and Tags Settings

Adding Tags to the Sidebar

EDITIONS

Available in: Salesforce Classic

Tag settings available in: **All** Editions

USER PERMISSIONS

To modify tag settings:
- Customize Application

When you enable tags for your organization, you can add the Tags component to your users' sidebar. This component allows users to navigate to the Tags page where they can browse, search, and manage their tags. It also lists each user's most recently used tags. To add this component:

1. From Setup, enter *Home Page Layouts* in the `Quick Find` box, then select **Home Page Layouts**.
2. Next to a home page layout that you want to modify, click **Edit**.
3. Select the `Tags` checkbox and click **Next**.
4. Arrange the Tags component on your page layout as desired, and click **Save**.

Tip: If you want the Tags component to appear on all pages and not just the Home tab, from Setup, enter *User Interface* in the `Quick Find` box, then select **User Interface**, and select `Show Custom Sidebar Components on All Pages`.

SEE ALSO:

Topics and Tags Settings

Delete Personal Tags for Deactivated Users

Your org can have up to 5,000,000 personal and public tags applied to records across all users. If your org is approaching this limit, delete personal tags for deactivated users.

1. From Setup, enter `Personal Tag Cleanup` in the `Quick Find` box, then select **Personal Tag Cleanup**.
2. Select one or more deactivated users and click **Delete**.

You can't restore personal tags after you delete them.

SEE ALSO:

Topics and Tags Settings

EDITIONS

Available in: Salesforce Classic

Personal Tag Cleanup available in: **All** Editions

USER PERMISSIONS

To delete personal tags for deactivated users:

- Customize Application

Control Who Sees What

Salesforce provides a flexible, layered data sharing design that allows you to expose different data sets to different sets of users, so users can do their job without seeing data they don't need to see. Use permission sets and profiles to specify the objects and fields users can access. Use organization-wide sharing settings, user roles, sharing rules to specify the individual records that users can view and edit.

EDITIONS

Available in: Salesforce Classic

The available data management options vary according to which Salesforce Edition you have.

Note: Who Sees What: Overview (English only)

Watch a demo on controlling access to and visibility of your data.

Tip: When implementing security and sharing rules for your organization, make a table of the various types of users in your organization. In the table, specify the level of access to data that each type of user needs for each object and for fields and records within the object. You can refer to this table as you set up your security model.

Object-Level Security (Permission Sets and Profiles)

Object-level security—or object permissions—provide the bluntest way to control data. Using object permissions you can prevent a user from seeing, creating, editing, or deleting any instance of a particular type of object, such as a lead or opportunity. Object permissions let you hide whole tabs and objects from particular users, so that they don't even know that type of data exists.

You specify object permissions in permission sets and profiles. *Permission sets* and *profiles* are collections of settings and permissions that determine what a user can do in the application, similar to a group in a Windows network, where all of the members of the group have the same folder permissions and access to the same software.

Profiles are typically defined by a user's job function (for example, system administrator or sales representative). A profile can be assigned to many users, but a user can be assigned to only one profile. You can use permission sets to grant additional permissions and access settings to users. It's easy to manage users' permissions and access with permission sets, because you can assign multiple permission sets to a single user.

Field-Level Security (Permission Sets and Profiles)

In some cases, you may want users to have access to an object, but limit their access to individual fields in that object. Field-level security—or field permissions—control whether a user can see, edit, and delete the value for a particular field on an object. They let you protect sensitive fields without having to hide the whole object from users. Field permissions are also controlled in permission sets and profiles.

Unlike page layouts, which only control the visibility of fields on detail and edit pages, field permissions control the visibility of fields in any part of the app, including related lists, list views, reports, and search results. To ensure that a user can't access a particular field, use field permissions. No other settings provide the same level of protection for a field.

Note: Field-level security doesn't prevent searching on the values in a field. When search terms match on field values protected by field-level security, the associated records are returned in the search results without the protected fields and their values.

Record-Level Security (Sharing)

After setting object- and field-level access permissions, you may want to configure access settings for the actual records themselves. Record-level security lets you give users access to some object records, but not others. Every record is owned by a user or a queue. The owner has full access to the record. In a hierarchy, users higher in the hierarchy always have the same access to users below them in the hierarchy. This access applies to records owned by users, as well as records shared with them.

To specify record-level security, set your organization-wide sharing settings, define a hierarchy, and create sharing rules.

- Organization-wide sharing settings—The first step in record-level security is to determine the organization-wide sharing settings for each object. Organization-wide sharing settings specify the default level of access users have to each others' records.

  You use organization-wide sharing settings to lock down your data to the most restrictive level, and then use the other record-level security and sharing tools to selectively give access to other users. For example, let's say users have object-level permissions to read and edit opportunities, and the organization-wide sharing setting is Read-Only. By default, those users can read all opportunity records, but can't edit any unless they own the record or are granted additional permissions.

- Role hierarchy—Once you've specified organization-wide sharing settings, the first way you can give wider access to records is with a role hierarchy. Similar to an organization chart, a role hierarchy represents a level of data access that a user or group of users needs. The role hierarchy ensures that users higher in the hierarchy always have access to the same data as people lower in their hierarchy, regardless of the organization-wide default settings. Role hierarchies don't have to match your organization chart exactly. Instead, each role in the hierarchy should represent a level of data access that a user or group of users needs.

  You can also use a territory hierarchy to share access to records. A territory hierarchy grants users access to records based on criteria such as zip code, industry, revenue, or a custom field that is relevant to your business. For example, you could create a territory hierarchy in which a user with the "North America" role has access to different data than users with the "Canada" and "United States" roles.

  Note: Although it's easy to confuse permission sets and profiles with roles, they control two very different things. Permission sets and profiles control a user's object and field access permissions. Roles primarily control a user's record-level access through role hierarchy and sharing rules.

- Sharing rules—Sharing rules let you make automatic exceptions to organization-wide sharing settings for particular sets of users, to give them access to records they don't own or can't normally see. Sharing rules, like role hierarchies, are only used to give additional users access to records—they can't be stricter than your organization-wide default settings.
- Manual sharing—Sometimes it's impossible to define a consistent group of users who need access to a particular set of records. In those situations, record owners can use manual sharing to give read and edit permissions to users who would not have access to the record any other way. Although manual sharing isn't automated like organization-wide sharing settings, role hierarchies, or sharing rules, it gives record owners the flexibility to share particular records with users that need to see them.
- Apex managed sharing—If sharing rules and manual sharing don't give you the control you need, you can use Apex managed sharing. Apex managed sharing allows developers to programmatically share custom objects. When you use Apex managed sharing to share a custom object, only users with the "Modify All Data" permission can add or change the sharing on the custom object's record, and the sharing access is maintained across record owner changes.

IN THIS SECTION:

Profiles

Profiles define how users access objects and data, and what they can do within the application. When you create users, you assign a profile to each one.

SEE ALSO:

Profiles

Permission Sets

Field-Level Security

Sharing Settings

User Permissions and Access

User permissions and access settings are specified in profiles and permission sets. To use them effectively, understand the differences between profiles and permission sets.

User permissions and access settings specify what users can do within an organization:

- Permissions determine a user's ability to edit an object record, view the Setup menu, empty the organizational Recycle Bin, or reset a user's password.
- Access settings determine other functions, such as access to Apex classes, app visibility, and the hours when users can log in.

Every user is assigned only one profile, but can also have multiple permission sets. When determining access for your users, use *profiles to assign the minimum permissions and access settings* for specific groups of users. Then use *permission sets to grant more permissions* as needed.

This table shows the types of permissions and access settings that are specified in profiles and permission sets.

Permission or Setting Type	In Profiles?	In Permission Sets?
Assigned apps	✓	✓
Tab settings	✓	✓
Record type assignments	✓	✓
Page layout assignments	✓	
Object permissions	✓	✓
Field permissions	✓	✓
User permissions (app and system)	✓	✓
Apex class access	✓	✓
Visualforce page access	✓	✓
External data source access	✓	✓

EDITIONS

Available in: Salesforce Classic and Lightning Experience

The available permissions and settings vary according to which Salesforce edition you have.

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

Permission or Setting Type	In Profiles?	In Permission Sets?
Service provider access (if Salesforce is enabled as an identity provider)	✓	✓
Custom permissions	✓	✓
Desktop client access	✓	
Login hours	✓	
Login IP ranges	✓	

SEE ALSO:

Profiles

Permission Sets

Revoking Permissions and Access

Profiles

Profiles define how users access objects and data, and what they can do within the application. When you create users, you assign a profile to each one.

Watch how you can grant users access to objects using profiles.

Who Sees What: Object Access (English only)

Your org includes several standard profiles where you can edit a limited number of settings. With editions that contain custom profiles, you can edit all permissions and settings except the user license. In Contact Manager, Essentials Edition, and Group Edition orgs, you can assign standard profiles to your users, but you can't view or edit the standard profiles, and you can't create custom profiles.

Every profile belongs to exactly one user license type.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

IN THIS SECTION:

Work in the Enhanced Profile User Interface Page

In the enhanced profile user interface, the profile overview page provides an entry point for all settings and permissions for a profile.

Work in the Original Profile Interface

To view a profile on the original profile page, from Setup, enter `Profiles` in the `Quick Find` box, then select **Profiles**, then select the profile you want.

Standard Profiles

Every org includes standard profiles that you can assign to users. In standard profiles, you can edit some settings.

Manage Profile Lists

Profiles define how users access objects and data, and what they can do within the application. When you create users, you assign a profile to each one. To view the profiles in your organization, from Setup, enter *Profiles* in the Quick Find box, then select **Profiles**.

Clone Profiles

Instead of creating profiles, save time by cloning existing profiles and customizing them.

Viewing a Profile's Assigned Users

To view all users that are assigned to a profile from the profile overview page, click **Assigned Users** (in the enhanced profile user interface) or **View Users** (in the original profile user interface). From the assigned users page, you can:

Edit Object Permissions in Profiles

Object permissions specify the type of access that users have to objects.

View and Edit Tab Settings in Permission Sets and Profiles

Tab settings specify whether a tab appears in the All Tabs page or is visible in a tab set.

View and Edit Assigned Apps in Profiles

Assigned app settings specify the apps that users can select in the Force.com app menu.

Enable Custom Permissions in Profiles

Custom permissions give you a way to provide access to custom processes or apps. After you've created a custom permission and associated it with a process or app, you can enable the permission in profiles.

View and Edit Session Timeout Settings in Profiles

Use Session Settings to set how many minutes or hours of inactivity elapse before a user's authentication session times out. At the end of the session, the user needs to log in again.

View and Edit Password Policies in Profiles

To ensure that the appropriate level of password security is used for your organization, specify password requirements with Password Policies settings for users assigned to a profile. Profile Password Policies settings override the organization-wide Password Policies for that profile's users. If you do not set Password Policies on a profile, the organization-wide Password Policies apply. New profile Password Policies take effect for existing profile users when they reset their passwords.

Password Policy Fields in Profiles

Specify password requirements with Password Policies settings. Refer to these field descriptions to understand how each one impacts a profile's password requirements.

Permission Sets

A permission set is a collection of settings and permissions that give users access to various tools and functions. The settings and permissions in permission sets are also found in profiles, but permission sets extend users' functional access without changing their profiles.

Permission Set Overview Page

App and System Settings in Permission Sets

In permission sets, permissions and settings are organized into app and system categories. These categories reflect the rights users need to administer and use system and app resources.

Search Permission Sets

To quickly navigate to other pages in a permission set, you can enter search terms in any permission set detail page.

View and Edit Assigned Apps in Permission Sets

Assigned app settings specify the apps that users can select in the Force.com app menu.

Assign Custom Record Types in Permission Sets

Enable Custom Permissions in Permission Sets

Custom permissions give you a way to provide access to custom processes or apps. After you've created a custom permission and associated it with a process or app, you can enable the permission in permission sets.

Manage Permission Set Assignments

You can assign permission sets to a single user from the user detail page or assign multiple users to a permission set from any permission set page.

SEE ALSO:

Edit Multiple Profiles with Profile List Views

Work in the Enhanced Profile User Interface Page

In the enhanced profile user interface, the profile overview page provides an entry point for all settings and permissions for a profile.

To open the profile overview page, from Setup, enter *Profiles* in the `Quick Find` box, then select **Profiles** and click the profile you want to view.

From the profile overview page, you can:

- Search for an object, permission, or setting
- Clone the profile
- If it's a custom profile, delete the profile by clicking **Delete**

  Note: You can't delete a profile that's assigned to a user, even if the user is inactive.

- Change the profile name or description by clicking **Edit Properties**
- View a list of users who are assigned to the profile
- Under Apps and System, click any of the links to view or edit permissions and settings.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view profiles:

- View Setup and Configuration

To delete profiles and edit profile properties:

- Manage Profiles and Permission Sets

IN THIS SECTION:

Enhanced Profile User Interface Overview

App and System Settings in the Enhanced Profile User Interface

Search in the Enhanced Profile User Interface

To locate an object, tab, permission, or setting name on a profile page, type at least three consecutive letters in the 🔍 **Find Settings** box. As you type, suggestions for results that match your search terms appear in a list. Click an item in the list to go to its settings page.

Working with Assigned Apps in the Enhanced Profile User Interface

Work with Object Settings in the Enhanced Profile User Interface

Assign Record Types and Page Layouts in the Enhanced Profile User Interface

App Permissions in the Enhanced Profile User Interface

Working with Apex Class Access in the Enhanced Profile User Interface

Working with Visualforce Page Access in the Enhanced Profile User Interface

System Permissions in the Enhanced Profile User Interface

Desktop Client Access in the Enhanced Profile User Interface

Working with Login Hours in the Enhanced Profile User Interface

View and Edit Login Hours in the Enhanced Profile User Interface
For each profile, you can specify the hours when users can log in.

Login IP Ranges in the Enhanced Profile User Interface

Restrict Login IP Ranges in the Enhanced Profile User Interface
Control login access at the user level by specifying a range of allowed IP addresses on a user's profile. When you define IP address restrictions for a profile, a login from any other IP address is denied.

Working with Service Provider Settings in the Enhanced Profile User Interface

SEE ALSO:

Enhanced Profile User Interface Overview

Enhanced Profile User Interface Overview

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To enable the enhanced profile user interface:

- Customize Application

The enhanced profile user interface provides a streamlined experience for managing profiles. With it, you can easily navigate, search, and modify settings for a profile.

To enable the enhanced profile user interface, from Setup, enter *`User Interface`* in the `Quick Find` box, then select **User Interface**, then select **Enable Enhanced Profile User Interface** and click **Save**. Your organization can only use one profile user interface at a time.

Note: You can't use the enhanced profile user interface if:

- You use Microsoft® Internet Explorer® 6 or earlier to manage your profiles (unless you've installed the Google Chrome Frame™ plug-in for Internet Explorer).
- Your organization uses category groups on guest profiles used for sites.
- Your organization delegates partner portal administration to portal users.

SEE ALSO:

Work in the Enhanced Profile User Interface Page

Profiles

App and System Settings in the Enhanced Profile User Interface

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

In the enhanced profile user interface, administrators can easily navigate, search, and modify settings for a single profile. Permissions and settings are organized into pages under app and system categories, which reflect the rights users need to administer and use app and system resources.

App Settings

Apps are sets of tabs that users can change by selecting the drop-down menu in the header. All underlying objects, components, data, and configurations remain the same, regardless of the selected app. In selecting an app, users navigate in a set of tabs that allows them to efficiently use the underlying functionality for app-specific tasks. For example, let's say you do most of your work in the sales app, which includes tabs like Accounts and Opportunities. To track a new marketing campaign, rather than adding the Campaigns tab to the sales app, you select Marketing from the app drop-down to view your campaigns and campaign members.

In the enhanced profile user interface, the Apps section of the overview page contains settings that are directly associated with the business processes that the apps enable. For example, customer service agents may need to manage cases, so the "Manage Cases" permission is in the Call Center section of the App Permissions page. Some app settings aren't related to app permissions. For example, to enable the Time-Off Manager app from the AppExchange, users need access to the appropriate Apex classes and Visualforce pages, as well as the object and field permissions that allow them to create new time-off requests.

Note: Regardless of the currently selected app, all of a user's permissions are respected. For example, although the "Import Leads" permission is under the Sales category, a user can import leads even while in the Service app.

System Settings

Some system functions apply to an organization and not to any single app. For example, login hours and login IP ranges control a user's ability to log in, regardless of which app the user accesses. Other system functions apply to all apps. For example, the "Run Reports" and "Manage Dashboards" permissions allow managers to create and manage reports in all apps. In some cases, such as with "Modify All Data," a permission applies to all apps, but also includes non-app functions, like the ability to download the Data Loader.

SEE ALSO:

Enhanced Profile User Interface Overview

Search in the Enhanced Profile User Interface

To locate an object, tab, permission, or setting name on a profile page, type at least three consecutive letters in the **Find Settings** box. As you type, suggestions for results that match your search terms appear in a list. Click an item in the list to go to its settings page.

Search terms aren't case-sensitive. For some categories, you can search for the specific permission or setting name. For other categories, search for the category name.

Item	Search for	Example
Assigned apps	App name	Type *`sales`* in the Find Settings box, then select `Sales` from the list.
Objects	Object name	Let's say you have an Albums custom object. Type *`albu`*, then select `Albums`.
• Fields • Record types • Page layout assignments	Parent object name	Let's say your Albums object contains a Description field. To find the `Description` field for albums, type *`albu`*, select `Albums`, and scroll down to `Description` under Field Permissions.
Tabs	Tab or parent object name	Type *`rep`*, then select `Reports`.
App and system permissions	Permission name	Type *`api`*, then select `API Enabled`.
All other categories	Category name	To find Apex class access settings, type *`apex`*, then select `Apex Class Access`. To find

EDITIONS

Available in: Salesforce Classic and Lightning Experience

The available profile permissions and settings vary according to which Salesforce edition you have.

USER PERMISSIONS

To find permissions and settings in a profile:

- View Setup and Configuration

Item	Search for	Example
		custom permissions, type *cust*, then select `Custom Permissions`. And so on.

If no results appear in a search:

- Check if the permission, object, tab, or setting you're searching for is available in the current organization.
- Verify that the item you're searching for is available for the user license that's associated with the current profile. For example, a profile with the High Volume Customer Portal license doesn't include the "Modify All Data" permission.
- Ensure that your search term contains at least three consecutive characters that match the name of the item you want to find.
- Make sure that you spelled the search term correctly.

SEE ALSO:

Enhanced Profile User Interface Overview

Assign Record Types and Page Layouts in the Enhanced Profile User Interface

In the enhanced profile user interface, Record Types and Page Layout Assignments settings determine the record type and page layout assignment mappings that are used when users view records. They also determine which record types are available when users create or edit records.

To specify record types and page layout assignments:

1. From Setup, enter *Profiles* in the `Quick Find` box, then select **Profiles**.
2. Select a profile.
3. In the **Find Settings...** box, enter the name of the object you want and select it from the list.
4. Click **Edit**.
5. In the Record Types and Page Layout Assignments section, make changes to the settings as needed.

Setting	Description
Record Types	Lists all existing record types for the object. `--Master--` is a system-generated record type that's used when a record has no custom record type associated with it. When `--Master--` is assigned, users can't set a record type to a record, such as during record creation. All other record types are custom record types.
Page Layout Assignment	The page layout to use for each record type. The page layout determines the buttons, fields, related lists, and other elements that users with this profile see when creating records with the associated record type. Since all users can access all record types, every record type must have a page layout assignment, even if the record type isn't specified as an assigned record type in the profile.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Record types available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To edit record type and page layout access settings:

- Manage Profiles and Permission Sets

Setting	Description
Assigned Record Types	Record types that are checked in this column are available when users with this profile create records for the object. If `--Master--` is selected, you can't select any custom record types; and if any custom record types are selected, you can't select `--Master--`.
Default Record Type	The default record type to use when users with this profile create records for the object.

The Record Types and Page Layout Assignments settings have some variations for the following objects or tabs.

Object or Tab	Variation
Accounts	If your organization uses person accounts, the accounts object additionally includes **Business Account Default Record Type** and **Person Account Default Record Type** settings, which specify the default record type to use when the profile's users create business or person account records from converted leads.
Cases	The cases object additionally includes **Case Close** settings, which show the page layout assignments to use for each record type on closed cases. That is, the same record type may have different page layouts for open and closed cases. With this additional setting, when users close a case, the case may have a different page layout that exposes how it was closed.
Home	You can't specify custom record types for the home tab. You can only select a page layout assignment for the --Master-- record type.

6. Click **Save**.

SEE ALSO:

How is record type access specified?

Assign Custom Record Types in Permission Sets

Work in the Enhanced Profile User Interface Page

View and Edit Login Hours in the Enhanced Profile User Interface

For each profile, you can specify the hours when users can log in.

1. From Setup, enter `Profiles` in the `Quick Find` box, then select **Profiles**.
2. Select a profile and click its name.
3. In the profile overview page, scroll down to Login Hours and click **Edit**.
4. Set the days and hours when users with this profile can log in to the organization.

   To allow users to log in at any time, click **Clear all times**. To prohibit users from using the system on a specific day, set the start and end times to the same value.

   If users are logged in when their login hours end, they can continue to view their current page, but they can't take any further action.

Note: The first time login hours are set for a profile, the hours are based on the organization's `Default Time Zone` as specified on the Company Information page in Setup. After that, any changes to the organization's `Default Time Zone` won't change the time zone for the profile's login hours. As a result, the login hours are always applied at those exact times even if a user is in a different time zone or if the organization's default time zone is changed.

Depending on whether you're viewing or editing login hours, the hours may appear differently. On the Login Hours edit page, hours are shown in your specified time zone. On the profile overview page, they appear in the organization's original default time zone.

SEE ALSO:

Enhanced Profile User Interface Overview

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view login hour settings:

- View Setup and Configuration

To edit login hour settings:

- Manage Profiles and Permission Sets

Restrict Login IP Ranges in the Enhanced Profile User Interface

Control login access at the user level by specifying a range of allowed IP addresses on a user's profile. When you define IP address restrictions for a profile, a login from any other IP address is denied.

1. From Setup, enter `Profiles` in the `Quick Find` box, then select **Profiles**.
2. Select a profile and click its name.
3. In the profile overview page, click **Login IP Ranges**.
4. Specify allowed IP addresses for the profile.
   - To add a range of IP addresses from which users can log in, click **Add IP Ranges**. Enter a valid IP address in the `IP Start Address` and a higher-numbered IP address in the `IP End Address` field. To allow logins from only a single IP address, enter the same address in both fields.
   - To edit or remove ranges, click **Edit** or **Delete** for that range.

   Important:

   - The IP addresses in a range must be either IPv4 or IPv6. In ranges, IPv4 addresses exist in the IPv4-mapped IPv6 address space `::ffff:0:0` to `::ffff:ffff:ffff`, where `::ffff:0:0` is `0.0.0.0` and `::ffff:ffff:ffff` is `255.255.255.255.` A range can't include IP addresses both inside and outside of the IPv4-mapped IPv6 address space. Ranges like `255.255.255.255` to `::1:0:0:0` or `::` to `::1:0:0:0` aren't allowed.
   - Partner User profiles are limited to five IP addresses. To increase this limit, contact Salesforce.
   - The Salesforce Mobile Classic app can bypass IP ranges that are defined for profiles. Salesforce Mobile Classic initiates a secure connection to Salesforce over the mobile carrier's network. However, the mobile carrier's IP addresses can be outside of the IP ranges allowed for the user's profile. To prevent bypassing IP definitions on a profile, disable Salesforce Mobile Classic on page 870 for that user.

5. Optionally enter a description for the range. If you maintain multiple ranges, use the Description field to provide details, like which part of your network corresponds to this range.

Note: You can further restrict access to Salesforce to only those IPs in Login IP Ranges. To enable this option, in Setup, enter *`Session Settings`* in the `Quick Find` box, then select **Session Settings** and select **Enforce login IP ranges on every request**. This option affects all user profiles that have login IP restrictions.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view login IP ranges:
- View Setup and Configuration

To edit and delete login IP ranges:
- Manage Profiles and Permission Sets

Work in the Original Profile Interface

To view a profile on the original profile page, from Setup, enter `Profiles` in the `Quick Find` box, then select **Profiles**, then select the profile you want.

On the profile detail page, you can:

- Edit the profile
- Create a profile based on this profile
- For custom profiles only, click **Delete** to delete the profile

  Note: You can't delete a profile that's assigned to a user, even if the user is inactive.

- View the users who are assigned to this profile

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

IN THIS SECTION:

Edit Profiles in the Original Profile Interface

Profiles define how users access objects and data and what they can do within the application. In standard profiles, you can edit a limited number of settings. In custom profiles, you can edit all available permissions and settings, except the user license.

Profile Settings in the Original Profile Interface

Profiles define how users access objects and data and what they can do within the application. View or edit these settings from the original profile detail page.

Assign Page Layouts in the Original Profile User Interface

If you're already working in an original profile user interface, you can access, view, and edit all page layout assignments easily in one location.

View and Edit Desktop Client Access in the Original Profile User Interface

Assign Record Types to Profiles in the Original Profile User Interface

After you create record types and include picklist values in them, add record types to user profiles. If you assign a default record type to a profile, users with that profile can assign the record type to records that they create or edit.

View and Edit Login Hours in the Original Profile User Interface

Specify the hours when users can log in based on the user profile.

Restrict Login IP Addresses in the Original Profile User Interface

Control login access at the user level by specifying a range of allowed IP addresses on a user's profile. When you define IP address restrictions for a profile, a login from any other IP address is denied.

Assign a Default Community to a User Profile

Assign a default community to a user profile to associate that profile with a specific community. The assigned community's branding is applied to email notifications about objects, which would otherwise be unbranded. Any links in the notification lead back to the default community—no more news from nowhere.

Edit Profiles in the Original Profile Interface

Profiles define how users access objects and data and what they can do within the application. In standard profiles, you can edit a limited number of settings. In custom profiles, you can edit all available permissions and settings, except the user license.

Note: Editing some permissions can result in enabling or disabling other ones. For example, enabling "View All Data" enables "Read" for all objects. Likewise, enabling "Transfer Leads" enables "Read" and "Create" on leads.

Tip: If enhanced profile list views are enabled for your organization, you can change permissions for multiple profiles from the list view.

1. From Setup, enter *Profiles* in the `Quick Find` box, then select **Profiles**.
2. Select the profile you want to change.
3. On the profile detail page, click **Edit**.

SEE ALSO:

Assign Page Layouts in the Original Profile User Interface

Profile Settings in the Original Profile Interface

View and Edit Desktop Client Access in the Original Profile User Interface

Assign Record Types to Profiles in the Original Profile User Interface

View and Edit Login Hours in the Original Profile User Interface

Restrict Login IP Addresses in the Original Profile User Interface

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To edit app and system permissions in profiles:

- Manage Profiles and Permission Sets

To edit app and system as well as object and field permissions in profiles:

- Manage Profiles and Permission Sets

  AND

  Customize Application

Profile Settings in the Original Profile Interface

Profiles define how users access objects and data and what they can do within the application. View or edit these settings from the original profile detail page.

Setting	To view or edit, go to
Profile name and description (custom profiles only)	Profile Detail
Administrative and general permissions (custom profiles only)	Administrative Permissions
App visibility settings	Custom App Settings
Console layouts for all profiles	Console Settings
Custom permissions	Enabled Custom Permissions
Desktop client access settings	Desktop Integration Clients
External data sources	Enabled External Data Source Access
Field access in objects	Field-Level Security
Login hours	Login Hours
Login IP address ranges	Login IP Ranges section, click **New**, or click **Edit** next to an existing IP range. Note: You can further restrict access to Salesforce to only those IPs in Login IP Ranges. To enable this option, in Setup, enter *`Session Settings`* in the `Quick Find` box, then select **Session Settings** and select **Enforce login IP ranges on every request**. This option affects all user profiles that have login IP restrictions.
Object permissions	Standard Object Permissions
Page layouts	Page Layouts
Record types	Record Type Settings section. You see the **Edit** link only if record types exist for the object.
Tab visibility settings	Tab Settings
Executable Apex classes	Enabled Apex Class Access
Executable Visualforce pages	Enabled Visualforce Page Access

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To edit profiles:

- Manage Profiles and Permission Sets

  AND

  Customize Application

Setting	To view or edit, go to
Service presence statuses	Enabled Service Presence Status Access

SEE ALSO:

Edit Profiles in the Original Profile Interface

Assign Page Layouts in the Original Profile User Interface

If you're already working in an original profile user interface, you can access, view, and edit all page layout assignments easily in one location.

1. From Setup, enter *Profiles* in the Quick Find box, then select **Profiles**.
2. Select a profile.
3. Click **View Assignment** next to any tab name in the Page Layouts section.
4. Click **Edit Assignment**.
5. Use the table to specify the page layout for each profile. If your organization uses record types, a matrix displays a page layout selector for each profile and record type.
   - Selected page layout assignments are highlighted.
   - Page layout assignments you change are italicized until you save your changes.
6. If necessary, select another page layout from the Page Layout To Use drop-down list and repeat the previous step for the new page layout.
7. Click **Save**.

SEE ALSO:

Work in the Original Profile Interface

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Record types available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To assign page layouts in profiles:

- Manage Profiles and Permission Sets

View and Edit Desktop Client Access in the Original Profile User Interface

Connect Offline and Connect for Office are desktop clients that integrate Salesforce with your PC. As an administrator, you can control which desktop clients your users can access as well as whether users are automatically notified when updates are available.

Note: To access desktop clients, users must also have the “API Enabled” permission.

1. From Setup, enter `Profiles` in the `Quick Find` box, then select **Profiles**.
2. Click **Edit** next to a profile name, and scroll to the Desktop Integration Clients section at the bottom of the page.

SEE ALSO:

Work in the Original Profile Interface

EDITIONS

Connect Offline available in: Salesforce Classic

Connect Offline available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Connect for Office available in: both Salesforce Classic and Lightning Experience

Connect for Office available in: **All** Editions except Database.com

USER PERMISSIONS

To view desktop client access settings:
- View Setup and Configuration

To edit desktop client access settings:
- Manage Profiles and Permission Sets

Assign Record Types to Profiles in the Original Profile User Interface

After you create record types and include picklist values in them, add record types to user profiles. If you assign a default record type to a profile, users with that profile can assign the record type to records that they create or edit.

Note: Users can view records of any record type, even if the record type is not associated with their profile.

You can associate several record types with a profile. For example, a user needs to create hardware and software sales opportunities. In this case, you can create and add both “Hardware” and “Software” record types to the user’s profile.

1. From Setup, enter `Profiles` in the `Quick Find` box, then select **Profiles**.
2. Select a profile. The record types available for that profile are listed in the Record Type Settings section.
3. Click **Edit** next to the appropriate type of record.
4. Select a record type from the Available Record Types list and add it to the Selected Record Types list.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To assign record types to profiles:
- Customize Application

Master is a system-generated record type that's used when a record has no custom record type associated with it. When you assign `Master`, users can't set a record type to a record, such as during record creation. All other record types are custom record types.

5. From `Default`, choose a default record type.

   If your organization uses person accounts, this setting also controls which account fields display in the `Quick Create` area of the accounts home page.

6. If your organization uses person accounts, set default record type options for both person accounts and business accounts. From the `Business Account Default Record Type` and then the `Person Account Default Record Type` drop-down list, choose a default record type.

   These settings are used when defaults are needed for both kinds of accounts, such as when converting leads.

7. Click **Save**.

Options in the Record Type Settings section are blank wherever no record types exist. For example, if you have two record types for opportunities but no record types for accounts, the **Edit** link only displays for opportunities. In this example, the picklist values and default value for the master are available in all accounts.

Note: If your organization uses person accounts, you can view the record type defaults for business accounts and person accounts. Go to Account Record Type Settings in the profile detail page. Clicking **Edit** in the Account Record Type Settings is another way to begin setting record type defaults for accounts.

SEE ALSO:

How is record type access specified?

Work in the Original Profile Interface

Assign Custom Record Types in Permission Sets

View and Edit Login Hours in the Original Profile User Interface

Specify the hours when users can log in based on the user profile.

1. From Setup, enter *`Profiles`* in the `Quick Find` box, then select **Profiles**, and select a profile.
2. Click **Edit** in the Login Hours related list.
3. Set the days and hours when users with this profile can use the system.

   To allow users to log in at any time, click **Clear All Times**. To prohibit users from using the system on a specific day, set the start and end times to the same value.

   If users are logged in when their login hours end, they can continue to view their current page, but they can't take any further action.

4. Click **Save**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To set login hours:

- Manage Profiles and Permission Sets

Note: The first time login hours are set for a profile, the hours are based on the organization's `Default Time Zone` as specified on the Company Information page in Setup. After that, any changes to the organization's `Default Time Zone` won't change the time zone for the profile's login hours. As a result, the login hours are always applied at those exact times even if a user is in a different time zone or if the organization's default time zone is changed.

Depending on whether you're viewing or editing login hours, the hours appear differently. On the profile detail page, hours are shown in your specified time zone. On the Login Hours edit page, they appear in the organization's default time zone.

SEE ALSO:

Work in the Original Profile Interface

Restrict Login IP Addresses in the Original Profile User Interface

Restrict Login IP Addresses in the Original Profile User Interface

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To view login IP ranges:
- View Setup and Configuration

To edit and delete login IP ranges:
- Manage Profiles and Permission Sets

Control login access at the user level by specifying a range of allowed IP addresses on a user's profile. When you define IP address restrictions for a profile, a login from any other IP address is denied.

1. How you restrict the range of valid IP addresses on a profile depends on your Salesforce edition.
   - If you're using an Enterprise, Unlimited, Performance, or Developer edition, from Setup, enter *`Profiles`* in the `Quick Find` box, then select **Profiles**, and select a profile.
   - If you're using a Professional, Group, or Personal edition, from Setup, enter *`Session Settings`* in the `Quick Find` box, then select **Session Settings**.
2. Click **New** in the Login IP Ranges related list.
3. Enter a valid IP address in the `IP Start Address` field and a higher-numbered IP address in the `IP End Address` field.

   The start and end addresses define the range of allowable IP addresses from which users can log in. To allow logins from a single IP address, enter the same address in both fields.
   - The IP addresses in a range must be either IPv4 or IPv6. In ranges, IPv4 addresses exist in the IPv4-mapped IPv6 address space `::ffff:0:0` to `::ffff:ffff:ffff`, where `::ffff:0:0` is `0.0.0.0` and `::ffff:ffff:ffff` is `255.255.255.255`. A range can't include IP addresses both inside and outside of the IPv4-mapped IPv6 address space. Ranges like `255.255.255.255` to `::1:0:0:0` or `::` to `::1:0:0:0` aren't allowed.
   - Partner User profiles are limited to five IP addresses. To increase this limit, contact Salesforce.
   - The Salesforce Mobile Classic app can bypass IP ranges that are defined for profiles. Salesforce Mobile Classic initiates a secure connection to Salesforce over the mobile carrier's network. However, the mobile carrier's IP addresses can be outside of the IP ranges allowed for the user's profile. To prevent bypassing IP definitions on a profile, disable Salesforce Mobile Classic on page 870 for that user.
4. Optionally enter a description for the range. If you maintain multiple ranges, use the Description field to provide details, such as which part of your network corresponds to this range.
5. Click **Save**.

Note: Cache settings on static resources are set to private when accessed via a Force.com site whose guest user's profile has restrictions based on IP range or login hours. Sites with guest user profile restrictions cache static resources only within the browser. Also, if a previously unrestricted site becomes restricted, it can take up to 45 days for the static resources to expire from the Salesforce cache and any intermediate caches.

Note: You can further restrict access to Salesforce to only those IPs in Login IP Ranges. To enable this option, in Setup, enter `Session Settings` in the `Quick Find` box, then select **Session Settings** and select **Enforce login IP ranges on every request**. This option affects all user profiles that have login IP restrictions.

SEE ALSO:

Set Trusted IP Ranges for Your Organization

View and Edit Login Hours in the Original Profile User Interface

Work in the Original Profile Interface

Assign a Default Community to a User Profile

EDITIONS

Available in: Lightning communities

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

USER PERMISSIONS

To assign a default community to a user profile:

- Chatter Enabled

  AND

  Create and Set Up Communities

Assign a default community to a user profile to associate that profile with a specific community. The assigned community's branding is applied to email notifications about objects, which would otherwise be unbranded. Any links in the notification lead back to the default community—no more news from nowhere.

Assign a **Default Community** value in Setup through Profiles.

1. In Setup, enter `Profiles` in the `Quick Find` box, then click **Profiles** in your results.
2. Click the name of the profile you want to change.
3. In the Default Community section, click **Edit**.
4. Select a community from the **Community** list.
5. Click **Save**.
   All community members who are assigned the user role are associated with the selected default community. When they receive email notifications about network-agnostic objects, like accounts, cases, and opportunities, the notifications are styled with the default community's brand. Links in the notifications email lead back to the default community.

Standard Profiles

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Your edition determines which standard profiles are available.

Every org includes standard profiles that you can assign to users. In standard profiles, you can edit some settings.

Every org includes standard profiles. In Professional, Enterprise, Unlimited, Performance, and Developer Editions, you can use standard profiles or create, edit, and delete custom profiles. In orgs where you can't create custom profiles (such as Contact Manager and Group Editions), you can assign standard profiles to your users, but you can't view or edit them.

The following table lists commonly used permissions in standard profiles.

Profile Name	Available Permissions
System Administrator	Can configure and customize the application. Has access to all functionality that does not require an additional license. For example, administrators cannot manage campaigns unless they also have a Marketing User license. Can manage price books and products. Can edit

Profile Name	Available Permissions
	any quota, override forecasts, and view any forecast.
Standard Platform User	Can use custom Force.com AppExchange apps developed in your org or installed from AppExchange. In addition, can use core platform functionality such as accounts, contacts, reports, dashboards, and custom tabs.
Standard Platform One App User	Can use one custom AppExchange app developed in your org or installed from AppExchange. The custom app is limited to five tabs. In addition, can use core platform functionality such as accounts, contacts, reports, dashboards, and custom tabs.
Standard User	Can create and edit most major types of records, run reports, and view the org's setup. Can view, but not manage, campaigns. Can create, but not review, solutions. Can edit personal quota and override forecasts.
Customer Community User	Can log in via a community. Your community settings and sharing model determine their access to tabs, objects, and other features. For more information, see Communities User Licenses.
Customer Community Plus User	
Partner Community User	
Customer Portal User	Can log in via a Customer Portal or a community. Can view and edit data they directly own or data owned by or shared with users below them in the Customer Portal role hierarchy; and they can view and edit cases where they are listed in the `Contact Name` field.
High Volume Customer Portal	Can log in via a Customer Portal or a community. The High Volume Customer Portal and Authenticated Website profiles are high-volume portal users.
Authenticated Website	
Customer Portal Manager	Can log in via a Customer Portal or a community. Can view and edit data they directly own or data owned by or shared with users below them in the Customer Portal role hierarchy; and they can view and edit cases where they are listed in the `Contact Name` field.
Partner User	Can log in via a partner portal or a community.
Solution Manager	Can review and publish solutions. Also has access to the same functionality as the Standard User.
Marketing User	Can manage campaigns, create letterheads, create HTML email templates, manage public documents, and add campaign members and update their statuses with the Data Import Wizard. Also has access to the same functionality as the Standard User.
Contract Manager	Can create, edit, activate, and approve contracts. This profile can also delete contracts as long as they are not activated. Can edit personal quota and override forecasts.

Profile Name	Available Permissions
Read Only	Can view the org's setup, run and export reports, and view, but not edit, other records.
Chatter Only User	Can only log in to Chatter. Can access all standard Chatter people, profiles, groups, and files. Additionally, they can: • View Salesforce accounts and contacts • Use Salesforce CRM Content, Ideas, and Answers • Access dashboards and reports • Use and approve workflows • Use the calendar to create and track activities • View and modify up to ten custom objects • Add records to groups Note: You must expose the tabs for the standard Salesforce objects that the Chatter Only user profile can access, as they are hidden by default for these users. Professional Edition organizations must have Profiles enabled to perform these tasks. Contact your Salesforce representative for more information. Only available with the Chatter Only user license. For more information on Chatter Plus users, see *Chatter Plus Frequently Asked Questions*.
Chatter Free User	Can only log in to Chatter. Can access all standard Chatter people, profiles, groups, and files. Only available with the Chatter Free user license.
Chatter External User	Can only log in to Chatter and access groups they've been invited to and interact with members of those groups. Only available with the Chatter External user license.
Chatter Moderator User	Can log in to Chatter. Can access all standard Chatter people, profiles, groups, and files. Additionally, this user can: • Activate and deactivate other Chatter Free users and moderators • Grant and revoke moderator privileges • Delete posts and comments that they can see • Edit their own posts and comments Note: Changing a user's profile from Chatter Moderator User to Chatter Free User removes moderator privileges in Chatter. Only available with the Chatter Free user license.

Profile Name	Available Permissions
Site.com Only User	Can only log in to the Site.com app. Each Site.com Only user also needs a Site.com Publisher feature license to create and publish sites, or a Site.com Contributor feature license to edit the site's content. Additionally, this user can: • Use one custom app with up to 20 custom objects • Access the Content app, but not the Accounts and Contacts objects • Create unlimited custom tabs Only available with the Site.com Only user license.

SEE ALSO:

Profiles

User Permissions

Manage Profile Lists

Profiles define how users access objects and data, and what they can do within the application. When you create users, you assign a profile to each one. To view the profiles in your organization, from Setup, enter `Profiles` in the `Quick Find` box, then select **Profiles**.

Viewing Enhanced Profile Lists

If enhanced profile list views are enabled for your organization, you can use additional tools to customize, navigate, manage, and print profile lists.

- Show a filtered list of profiles by selecting a view from the drop-down list.
- Delete a view by selecting it from the drop-down list and clicking **Delete**.
- Create a list view or edit an existing view.
- Create a profile.
- Print the list view by clicking 🖨.
- Refresh the list view after creating or editing a view by clicking 🔄.
- Edit permissions directly in the list view.
- View or edit a profile by clicking its name.
- Delete a custom profile by clicking **Del** next to its name.

  Note: You can't delete a profile that's assigned to a user, even if the user is inactive.

Viewing the Basic Profile List

- Create a profile.
- View or edit a profile by clicking its name.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view profiles, and print profile lists:

- View Setup and Configuration

To delete profile list views:

- Manage Profiles and Permission Sets

To delete custom profiles:

- Manage Profiles and Permission Sets

- Delete a custom profile by clicking **Del** next to its name.

IN THIS SECTION:

Creating and Editing Profile List Views

Edit Multiple Profiles with Profile List Views

If enhanced profile list views are enabled for your organization, you can change permissions in up to 200 profiles directly from the list view, without accessing individual profile pages.

SEE ALSO:

Edit Multiple Profiles with Profile List Views

Profiles

Creating and Editing Profile List Views

If enhanced profile list views are enabled for your organization, you can create profile list views to show a set of profiles with the fields you choose. For example, you could create a list view of all profiles in which "Modify All Data" is enabled.

1. In the Profiles page, click **Create New View**, or select a view and click **Edit**.
2. Enter the view name.
3. Under Specify Filter Criteria, specify the conditions that the list items must match, such as *`Modify All Data equals True`*.
   a. Type a setting name, or click the lookup icon 🔍 to search for and select the setting you want.
   b. Choose a filter operator.
   c. Enter the value that you want to match.
   d. To specify another filter condition, click **Add New**. You can specify up to 25 filter condition rows.

      To remove a filter condition row and clear its values, click the remove row icon ✕.
4. Under Select Columns to Display, specify the profile settings that you want to appear as columns in the list view.
   a. From the Search drop-down list, select the type of setting you want to search for.
   b. Enter part or all of a word in the setting you want to add and click **Find**.

      Note: If the search finds more than 500 values, no results appear. Use the preceding steps to refine your search criteria and show fewer results.
   c. To add or remove columns, select one or more column names and click the **Add** or **Remove** arrow.
   d. Use the **Top**, **Up**, **Down**, and **Bottom** arrows to arrange the columns in the sequence you want.

   You can add up to 15 columns in a single list view.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To create, edit, and delete profile list views:

- Manage Profiles and Permission Sets

5. Click **Save**, or if you're cloning an existing view, rename it and click **Save As**.

SEE ALSO:

Edit Multiple Profiles with Profile List Views

Edit Multiple Profiles with Profile List Views

If enhanced profile list views are enabled for your organization, you can change permissions in up to 200 profiles directly from the list view, without accessing individual profile pages.

Editable cells display a pencil icon (✎) when you hover over the cell, while non-editable cells display a lock icon (🔒). In some cases, such as in standard profiles, the pencil icon appears but the setting is not actually editable.

Warning: Use care when editing profiles with this method. Because profiles affect a user's fundamental access, making mass changes may have a widespread effect on users in your organization.

1. Select or create a list view that includes the profiles and permissions you want to edit.
2. To edit multiple profiles, select the checkbox next to each profile you want to edit.

   If you select profiles on multiple pages, Salesforce remembers which profiles are selected.
3. Double-click the permission you want to edit.

   For multiple profiles, double-click the permission in any of the selected profiles.
4. In the dialog box that appears, enable or disable the permission.

   In some cases, changing a permission may also change other permissions. For example, if "Customize Application" and "View Setup and Configuration" are disabled and you enable "Customize Application," then "View Setup and Configuration" is also enabled. In this case, the dialog box lists the affected permissions.
5. To change multiple profiles, select **All** *n* **selected records** (where *n* is the number of profiles you selected).
6. Click **Save**.

Note:

- For standard profiles, inline editing is available only for the "Single Sign-On" and "Affected By Divisions" permissions.
- If you edit multiple profiles, only those profiles that support the permission you are changing will change. For example, if you use inline editing to add "Modify All Data" to multiple profiles, but because of its user license the profile doesn't have "Modify All Data," the profile won't change.

If any errors occur, an error message appears, listing each profile in error and a description of the error. Click the profile name to open the profile detail page. The profiles you've clicked appear in the error window in gray, strike-through text. To view the error console, you must have pop-up blockers disabled for the Salesforce domain.

Any changes you make are recorded in the setup audit trail.

SEE ALSO:

Profiles

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit multiple profiles from the list view:

- Manage Profiles and Permission Sets

  AND

  Customize Application

Clone Profiles

Instead of creating profiles, save time by cloning existing profiles and customizing them.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To create profiles:

- Manage Profiles and Permission Sets

Tip: If you clone profiles to enable certain permissions or access settings, consider using permission sets. For more information, see Permission Sets. Also, if your profile name contains more than one word, avoid extraneous spacing. For example, “Acme User” and “Acme User” are identical other than spacing between “Acme” and “User.” Using both profiles in this case can result in confusion for admins and users.

1. From Setup, enter `Profiles` in the `Quick Find` box, then select **Profiles**.
2. In the Profiles list page, do one of the following:
   - Click **New Profile**, then select an existing profile that’s similar to the one you want to create.
   - If enhanced profile list views are enabled, click **Clone** next to a profile that’s similar to the one you want to create.
   - Click the name of a profile that’s similar to the one you want to create, then in the profile page, click **Clone**.

   A new profile uses the same user license as the profile it was cloned from.
3. Enter a profile name.
4. Click **Save**.

SEE ALSO:

Profiles

Viewing a Profile's Assigned Users

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

To view all users that are assigned to a profile from the profile overview page, click **Assigned Users** (in the enhanced profile user interface) or **View Users** (in the original profile user interface). From the assigned users page, you can:

- Create one or multiple users
- Reset passwords for selected users
- Edit a user
- View a user's detail page by clicking the name, alias, or username
- View or edit a profile by clicking the profile name
- If Google Apps™ is enabled in your organization, export users to Google and create Google Apps accounts by clicking **Export to Google Apps**

SEE ALSO:

Profiles

Edit Object Permissions in Profiles

Object permissions specify the type of access that users have to objects.

1. From Setup, either:
   - Enter `Permission Sets` in the `Quick Find` box, then select **Permission Sets**, or
   - Enter `Profiles` in the `Quick Find` box, then select **Profiles**
2. Select a permission set or profile.
3. Depending on which interface you're using, do one of the following:
   - Permission sets or enhanced profile user interface—In the **Find Settings...** box, enter the name of the object and select it from the list. Click **Edit**, then scroll to the Object Permissions section.
   - Original profile user interface—Click **Edit**, then scroll to the Standard Object Permissions, Custom Object Permissions, or External Object Permissions section.
4. Specify the object permissions.
5. Click **Save**.

SEE ALSO:

Object Permissions

Profiles

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view object permissions:
- View Setup and Configuration

To edit object permissions:
- Manage Profiles and Permission Sets

  AND

  Customize Application

View and Edit Tab Settings in Permission Sets and Profiles

Tab settings specify whether a tab appears in the All Tabs page or is visible in a tab set.

1. From Setup, either:
   - Enter `Permission Sets` in the `Quick Find` box, then select **Permission Sets**, or
   - Enter `Profiles` in the `Quick Find` box, then select **Profiles**
2. Select a permission set or profile.
3. Do one of the following:
   - Permission sets or enhanced profile user interface—In the **Find Settings...** box, enter the name of the tab you want and select it from the list, then click **Edit**.
   - Original profile user interface—Click **Edit**, then scroll to the Tab Settings section.
4. Specify the tab settings.
5. (Original profile user interface only) To reset users' tab customizations to the tab visibility settings that you specify, select **Overwrite users' personal tab customizations**.
6. Click **Save**.

Note: If Salesforce CRM Content is enabled for your organization but the **Salesforce CRM Content User** checkbox isn't enabled on the user detail page, the Salesforce CRM Content app has no tabs.

IN THIS SECTION:

Tab Settings

Tab settings specify whether a tab appears in the All Tabs page or is visible in its associated app. They also determine whether objects appear in the Lightning Experience App Launcher and navigation menus. Tab settings labels in permission sets differ from the labels in profiles.

SEE ALSO:

Profiles

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Tab settings available in: **All** Editions except **Database.com**

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

Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

USER PERMISSIONS

To view tab settings:

- View Setup and Configuration

To edit tab settings:

- Manage Profiles and Permission Sets

Tab Settings

Tab settings specify whether a tab appears in the All Tabs page or is visible in its associated app. They also determine whether objects appear in the Lightning Experience App Launcher and navigation menus. Tab settings labels in permission sets differ from the labels in profiles.

Enabled Settings in Permission Sets	Enabled Setting in Profiles	Description
`Available`	`Default Off`	The tab is available on the All Tabs page. Individual users can customize their display to make the tab visible in any app.
`Available` and `Visible`	`Default On`	The tab is available on the All Tabs page and appears in the visible tabs for its associated app. In Lightning Experience, this setting determines whether an object appears in the App Launcher and in navigation menus. Individual users can customize their display to hide the tab or make it visible in other apps.
None	`Tab Hidden`	The tab isn't available on the All Tabs page or visible in any apps.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Tab settings available in: **All** Editions except **Database.com**

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

Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Note: If a user has another permission set or profile with enabled settings for the same tab, the most permissive setting applies. For example, let's say permission set A has no settings enabled for the Accounts tab, and permission set B enables the `Available` setting for the Accounts tab. If permission sets A and B are assigned to a user, the user sees the Accounts tab on the All Tabs page.

SEE ALSO:

View and Edit Tab Settings in Permission Sets and Profiles

View and Edit Assigned Apps in Profiles

Assigned app settings specify the apps that users can select in the Force.com app menu.

Every profile must have at least one visible app, except profiles associated with Customer Portal users because apps are not available to them.

To specify app visibility:

1. From Setup, enter `Profiles` in the `Quick Find` box, then select **Profiles**.
2. Select a profile.
3. Depending on which user interface you're using, do one of the following:
   - Enhanced profile user interface—Click **Assigned Apps**, then click **Edit**.
   - Original profile user interface—Click **Edit**, then scroll to the Custom App Settings section.
4. Select one default app. The default app appears when users log in for the first time.
5. Select **Visible** for any other apps you want to make visible.

SEE ALSO:

Profiles

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To edit app visibility settings:

- Manage Profiles and Permission Sets

Enable Custom Permissions in Profiles

Custom permissions give you a way to provide access to custom processes or apps. After you've created a custom permission and associated it with a process or app, you can enable the permission in profiles.

1. From Setup, enter `Profiles` in the `Quick Find` box, then select **Profiles**.
2. Select a profile.
3. Depending on which user interface you're using, do one of the following.
   - Enhanced profile user interface: Click **Custom Permissions**, and then click **Edit**.
   - Original profile user interface: In the Enabled Custom Permissions related list, click **Edit**.
4. To enable custom permissions, select them from the Available Custom Permissions list and click **Add**. To remove custom permissions from the profile, select them from the Enabled Custom Permissions list and click **Remove**.
5. Click **Save**.

SEE ALSO:

Custom Permissions

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

In Group and Professional Edition organizations, you can't create or edit custom permissions, but you can install them as part of a managed package.

USER PERMISSIONS

To enable custom permissions in profiles:

- Manage Profiles and Permission Sets

View and Edit Session Timeout Settings in Profiles

Use Session Settings to set how many minutes or hours of inactivity elapse before a user's authentication session times out. At the end of the session, the user needs to log in again.

Until you set the `Session times out after` value on a profile, the `Timeout value` in the organization Session Settings applies to users of the profile. When set, the profile `Session times out after` value overrides the org-wide `Timeout value`. Changes to the org-wide `Timeout value` don't apply to users of a profile with its own `Session times out after` value.

1. From Setup, enter *`Profiles`* in the `Quick Find` box, then select **Profiles**.
2. Select a profile.
3. Depending on which user interface you're using, do one of the following.
   - Enhanced profile user interface—Click **Session Settings**, then click **Edit**.
   - Original profile user interface—Click **Edit**, then scroll to the Session Settings section.
4. Select a timeout value from the drop-down list.
5. Click **Save**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To edit session and password settings in profiles:

- Manage Profiles and Permission Sets

View and Edit Password Policies in Profiles

To ensure that the appropriate level of password security is used for your organization, specify password requirements with Password Policies settings for users assigned to a profile. Profile Password Policies settings override the organization-wide Password Policies for that profile's users. If you do not set Password Policies on a profile, the organization-wide Password Policies apply. New profile Password Policies take effect for existing profile users when they reset their passwords.

Changes to the organization-wide Password Policies don't apply to users of a profile with its own Password Policies.

1. From Setup, enter `Profiles` in the `Quick Find` box, then select **Profiles**.
2. Select a profile.
3. Depending on which user interface you're using, do one of the following.
   - Enhanced profile user interface—Click **Password Policies**, then click **Edit**.
   - Original profile user interface—Click **Edit**, then scroll to the Password Policies section.
4. Change the values for the profile.

   Note: If you change the `User passwords expire in` setting, the change affects a user's password expiration date if that user's new expiration date is earlier than the old expiration date or if you remove an expiration by selecting `Never expires`.
5. Click **Save**.

SEE ALSO:

Password Policy Fields in Profiles

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To edit session and password settings in profiles:
- Manage Profiles and Permission Sets

To set password policies:
- Manage Password Policies

Password Policy Fields in Profiles

Specify password requirements with Password Policies settings. Refer to these field descriptions to understand how each one impacts a profile's password requirements.

Changes to the organization-wide password policies don't apply to users of a profile with its own password policies.

Field	Description
`User passwords expire in`	The length of time until user passwords expire and must be changed. The default is 90 days. This setting isn't available for Self-Service portals. This setting doesn't apply to users with the "Password Never Expires" permission. If you change the `User passwords expire in` setting, the change affects a user's password expiration date if that user's new expiration date is earlier than the old expiration date or if you remove an expiration by selecting `Never expires`.
`Enforce password history`	Save users' previous passwords so that they must always reset their password to a new, unique password. Password history is not saved until you set this value. The default is `3 passwords remembered`. You cannot select `No passwords`

Field	Description
	`remembered` unless you select `Never expires` for the `User passwords expire in` field. This setting isn't available for Self-Service portals.
`Minimum password length`	The minimum number of characters required for a password. When you set this value, existing users aren't affected until the next time they change their passwords. The default is `8 characters`.
`Password complexity requirement`	The requirement for which types of characters must be used in a user's password. Complexity levels: - `No restriction`—allows any password value and is the least secure option. - `Must mix alpha and numeric characters`—requires at least one alphabetic character and one number, which is the default. - `Must mix alpha, numeric, and special characters`—requires at least one alphabetic character, one number, and one of the following special characters: `! # $ % - _ = + < >`. - `Must mix numbers and uppercase and lowercase letters`—requires at least one number, one uppercase letter, and one lowercase letter. - `Must mix numbers, uppercase and lowercase letters, and special characters`—requires at least one number, one uppercase letter, and one lowercase letter, and one of the following special characters: `! # $ % - _ = + < >`. Note: Only the special characters listed meet the requirement. Other symbol characters are not considered special characters.
`Password question requirement`	The values are `Cannot contain password`, meaning that the answer to the password hint question cannot contain the password itself; or `None`, the default, for no restrictions on the answer. The user's answer to the password hint question is required. This setting is not available for Self-Service portals, Customer Portals, or partner portals.
`Maximum invalid login attempts`	The number of login failures allowed for a user before they become locked out. This setting isn't available for Self-Service portals.
`Lockout effective period`	The duration of the login lockout. The default is 15 minutes. This setting isn't available for Self-Service portals. Note: If users are locked out, they must wait until the lockout period expires. Alternatively, a user with the "Reset

Field	Description
	User Passwords and Unlock Users” permission can unlock them from Setup with the following procedure: 1. Enter *`Users`* in the `Quick Find` box. 2. Select **Users**. 3. Selecting the user. 4. Click **Unlock**. This button is only available when a user is locked out.
`Obscure secret answer for password resets`	This feature hides answers to security questions as you type. The default is to show the answer in plain text. Note: If your org uses the Microsoft Input Method Editor (IME) with the input mode set to Hiragana, when you type ASCII characters, they’re converted in Japanese characters in normal text fields. However, the IME doesn’t work properly in fields with obscured text. If your org’s users cannot properly enter their passwords or other values after enabling this feature, disable the feature.
`Require a minimum 1 day password lifetime`	When you select this option, a password can’t be changed more than once in a 24-hour period.

SEE ALSO:

View and Edit Password Policies in Profiles

Permission Sets

A permission set is a collection of settings and permissions that give users access to various tools and functions. The settings and permissions in permission sets are also found in profiles, but permission sets extend users’ functional access without changing their profiles.

Users can have only one profile but, depending on the Salesforce edition, they can have multiple permission sets. You can assign permission sets to various types of users, regardless of their profiles.

Create permission sets to grant access among logical groupings of users, regardless of their primary job function. For example, let’s say you have several users with a profile called Sales User. This profile allows assignees to read, create, and edit leads. Some, but not all, of these users also need to delete and transfer leads. Instead of creating another profile, create a permission set.

Sales User profile
Read, create, and edit leads
Additional lead permissions
+ Delete Leads
+ Transfer Leads

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Or, let's say you have an Inventory custom object in your org. Many users need "Read" access to this object, and a smaller number of users need "Edit" access. You can create a permission set that grants "Read" access and assign it to the appropriate users. You can then create another permission set that gives "Edit" access to the Inventory object and assign it to the smaller group of users.

If a permission isn't enabled in a profile but is enabled in a permission set, users with that profile and permission set have the permission. For example, if "Manage Password Policies" isn't enabled in Jane Smith's profile but is enabled in one of her permission sets, she can manage password policies.

IN THIS SECTION:

Create Permission Sets

You can clone a permission set or create a new one. A cloned permission set starts with the same licenses and enabled permissions as the original one. A new permission set starts with no licenses selected and no permissions enabled.

1. From Setup, enter *Permission Sets* in the `Quick Find` box, then select **Permission Sets**.
2. Click **New**.
3. Enter your permission set information.
4. Select the types of users for the permission set.

   When you create a permission set, you select a specific user or permission set license. If only users with one type of license can use the permission set, select the license that's associated with the users. For example, to create a permission set for users with

   - the Salesforce license, select Salesforce. You can enable permissions only allowed in the Salesforce license.
   - the Identity Connect permission set license, select Identity Connect. You can enable permissions only allowed in the Identity Connect license.
   - different licenses, select **None**. Not selecting a specific license allows you to assign the permission set to any user whose license allows the permissions you enable in the permission

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create permission sets:
- "Manage Profiles and Permission Sets"

To assign permission sets:
- "Assign Permission Sets"

set. For example, to assign the permission set to users with the Salesforce license and to users with the Salesforce Platform license, select **None**.

When creating a permission set for a specific permission set license, refer to that feature's documentation. For example, to create a permission set for the Identity Connect permission set license, use these steps along with the Identity Connect documentation.

Example: Let's say you have several users with a profile called Sales User. This profile allows assignees to read, create, and edit leads. But you need some users to also delete and transfer leads. On the permission set page that you create, go to Find Settings and begin typing `Lead`. Under Object Settings, select **Leads** and enable delete. "Transfer Leads" is an app permission (rather than object permission). To enable it, in Find Settings, begin typing `leads`. "Transfer Leads" is listed under App Permissions. Assign the permission set to users who need these permissions.

Note:

- Permission sets with no license selected don't include all possible permissions and settings.
- Assign a permission set with no license only to users whose user licenses allow the permissions and settings that you are enabling in the permission set. For example, don't create a permission set with no user license and then enable "Author Apex" and assign it to Salesforce Platform users. You can't assign this permission set to Salesforce Platform users because the Salesforce Platform user license doesn't allow Apex authoring.

SEE ALSO:

Permission Sets

Standard Permission Sets

Assign a Feature Permission Set License and Permission Set

What Are Permission Set Licenses?

Assign Permission Sets to a Single User

Assign permission sets or remove permission set assignments for a single user from the user detail page.

The Permission Set Assignments page shows:

- Permission sets with no associated license. For example, you can assign a permission set if **None** was selected for the license type in the permission set. Make sure that the user's license allows all the permission set's enabled settings and permissions. If the user's license doesn't allow selected permissions, the assignment fails.
- Permission sets that match the user's license. For example, if a user's license is Chatter Only, you can assign permission sets with the Chatter Only license.
- Permission sets specific to permission set licenses. Let's say you create a permission set named Identity and associate that permission set to the "Identity Connect" permission set license. When you assign users to Identity, they receive all functionality available with the Identity Connect permission set license.

Note: Some permissions require users to have a permission set license before you can grant the permissions. For example, if you add the "Use Identity Connect" user permission to the Identity permission set, you can assign only users with the Identity Connect permission set license to the permission set.

1. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.
2. Select a user.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To assign permission sets:

- "Assign Permission Sets"

3. In the Permission Set Assignments related list, click **Edit Assignments**.
4. To assign a permission set, select it under Available Permission Sets and click **Add**. To remove a permission set assignment, select it under Enabled Permission Sets and click **Remove**.
5. Click **Save**.

Tip: You can perform this and other administration tasks from the SalesforceA mobile app.

SEE ALSO:

- Assign a Permission Set to Multiple Users
- Standard Permission Sets
- Help Users From Anywhere With SalesforceA
- Assign a Permission Set to Multiple Users

Standard Permission Sets

A standard permission set consists of a group of common permissions for a particular feature associated with a permission set license. Using a standard permission set saves you time and facilitates administration because you don't need to create the custom permission set.

The following permission set license comes with a standard permission set. To enable specific features, refer to that feature's documentation.

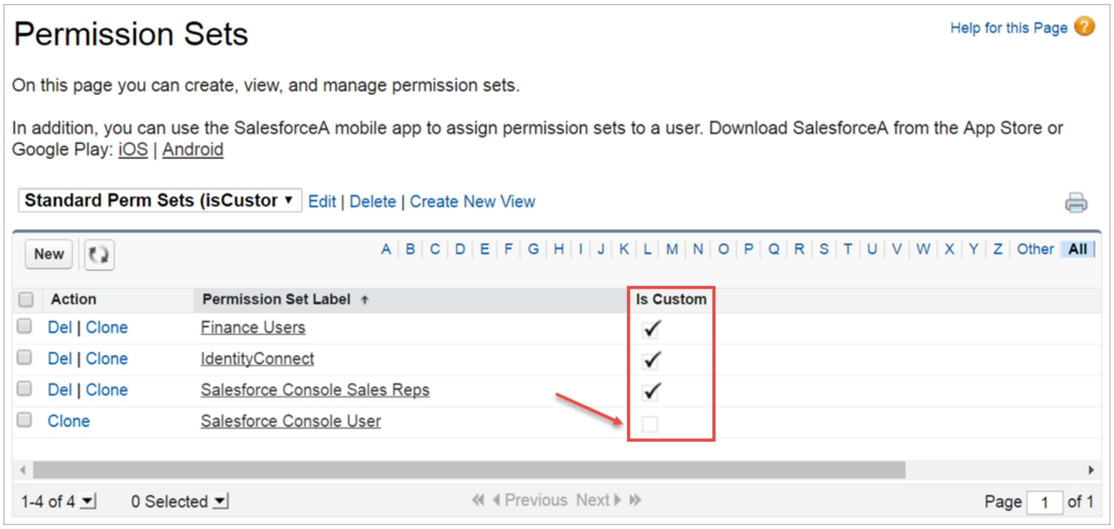
Permission Set License Name	Permission Set Name
Sales Console User in Salesforce Classic	Salesforce Console User in Salesforce Classic

To see which permission sets are standard, add `Is Custom` to your list view. The Is Custom box isn't checked for standard permission set. Permission sets you created or cloned are indicated with a checkmark.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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



Permission Sets

On this page you can create, view, and manage permission sets.

In addition, you can use the SalesforceA mobile app to assign permission sets to a user. Download SalesforceA from the App Store or Google Play: iOS | Android

Standard Perm Sets (isCustor ▾ Edit | Delete | Create New View

☐	Action	Permission Set Label ↑	Is Custom
☐	Del | Clone	Finance Users	✓
☐	Del | Clone	IdentityConnect	✓
☐	Del | Clone	Salesforce Console Sales Reps	✓
☐	Clone	Salesforce Console User	☐

1-4 of 4 0 Selected Page 1 of 1

Help for this Page
New
A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | Other | All
Previous Next

Standard permission sets don't count against your org's permission set limits. You can clone a standard permission set as many times as you want, but you can't edit it. Clones do count against your org's permission set limits.

Example: Let's say you purchased 10 Sales Console User permission set licenses. You can do any of the following.

- Assign all 10 users to the Salesforce Console User permission set.
- Assign some of the users to the Salesforce Console User permission set, and assign the remainder to a clone of Salesforce Console User.
- Clone the Salesforce Console User permission set and assign different users to each clone, based on your org's structure.

Session-based Permission Sets

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Create session-based permission sets that allow access only during specified sessions. For example, create a session-based permission set that grants access to an application only during an authenticated session.

IN THIS SECTION:

What Are Session-Based Permission Sets?

Session-based permission sets apply to a specific session. Understand why and when to create a session-based permission set.

Create a Flow That Can Activate or Deactivate a Session-Based Permission Set

You can create a session-based permission set and then create a flow that users can run to activate or deactivate the permission set themselves.

What Are Session-Based Permission Sets?

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Session-based permission sets apply to a specific session. Understand why and when to create a session-based permission set.

Use a session-based permission set to allow functional access only during a predefined session type. For example, let's say your org has a custom object called Conference Room. A mobile app called Conference Room Sync has read and update access to the object. You can create a permission set to allow updates to the object only when the Conference Room Sync connected mobile app generates the user's session.

In another example, you have a web application that accesses confidential information. For security, you want to limit user access to specific types of sessions for a predetermined length of time. You can create a session-based permission set that activates only when users authenticate into your environment using a token. When the token expires, the user must reauthenticate to access the application again.

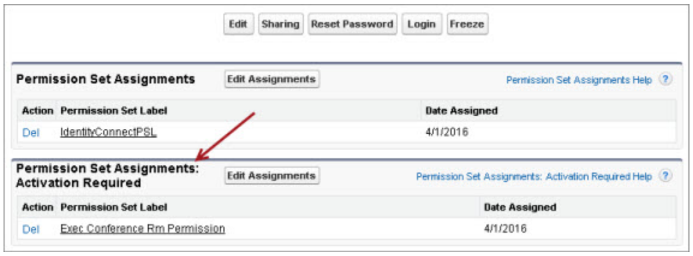
For this example, you have a junior buyer in your org who occasionally requires access to your Contracts object. Create a session-based permission set with access to the object, and then create a flow that uses the Activate Session-Based Permission Set action available in the Cloud Flow Designer. In the flow, pass the permission name to the action. During runtime, the action checks who's running the flow. When the junior buyer runs the flow, the activation process fires. When the flow completes, the buyer has access to the Contracts object for the current session.

To activate session-based permission sets via the SOAP API, see the SessionPermSetActivation object in the SOAP API Developer Guide. You need the Manage Session Permission Set Activation permission.

Before assigning session-based permission sets to users, ensure that they can meet the conditions of the permission set. For example, grant user access to appropriate tools, such as authenticators. As a best practice, inform users of the conditions in which they can access certain applications and tools.

Tip: When you create your permission set list view, select columns to include **Session Activation Required** to view which permission sets are session-based.

User assignment information appears on the user detail page in a related list called Permission Set Assignments: Activation Required.


Edit
Sharing
Reset Password
Login
Freeze
Edit Assignments
Permission Set Assignments Help
Edit Assignments
Permission Set Assignments: Activation Required Help

Permission Set Assignments

Action	Permission Set Label	Date Assigned
Del	IdentityConnectPSL	4/1/2016

Permission Set Assignments: Activation Required

Action	Permission Set Label	Date Assigned
Del	Exec Conference Rm Permission	4/1/2016

SEE ALSO:

Permission Sets

Create a Flow That Can Activate or Deactivate a Session-Based Permission Set

Create a Flow That Can Activate or Deactivate a Session-Based Permission Set

You can create a session-based permission set and then create a flow that users can run to activate or deactivate the permission set themselves.

Before beginning, check out What Are Session-Based Permission Sets? to learn when to use them.

Important: You can run queries, however, do not make data or object updates in flows that also activate session-based permission sets.

1. Create a permission set and make sure to select **Session Activation Required**
2. Assign the permission set to users.
3. Create a flow.
    a. In the Cloud Flow Designer, select the **Activate Session-Based Permission Set** or **Deactivate Session-Based Permission Set** action. Descriptions of the actions are in the palette.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

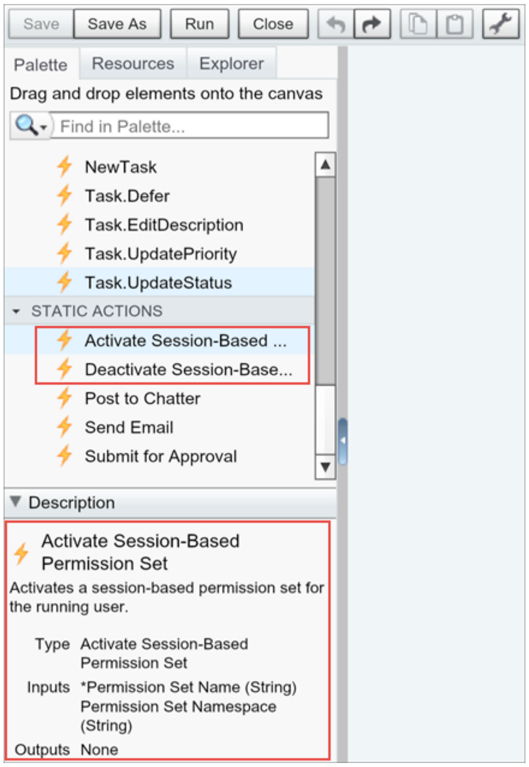
Available in: **Contact Manager**, **Professional**, **Group**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

USER PERMISSIONS

To create permission sets:
- Manage Profiles and Permission Sets

To assign permission sets:
- Assign Permission Sets

To open, edit, or create a flow in the Cloud Flow Designer:
- Manage Force.com Flow



Activate Session-Based Permission Set

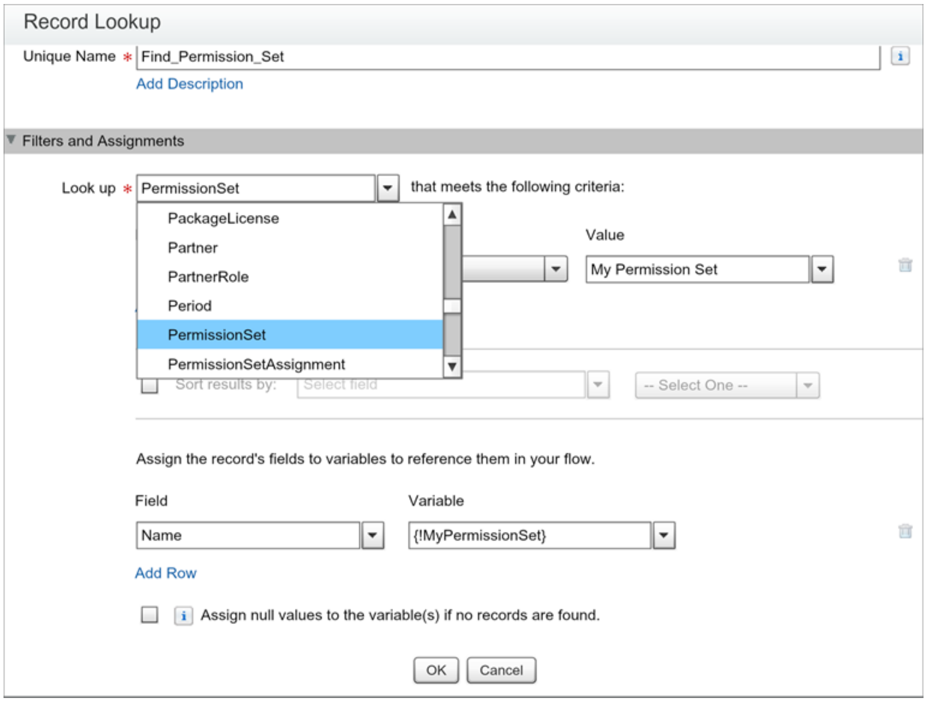
Activates a session-based permission set for the running user.

Type: Activate Session-Based Permission Set

Inputs: *Permission Set Name (String)
Permission Set Namespace (String)

Outputs: None

b. In the flow, pass the permission name to the action.



Unique Name * Find_Permission_Set

Look up * PermissionSet that meets the following criteria:

Value: My Permission Set

Assign the record's fields to variables to reference them in your flow.

Field	Variable
Name	{!MyPermissionSet}

□ Assign null values to the variable(s) if no records are found.

4. Activate your flow.

5. Distribute your flow to users who need to run it.

Example: Create a flow to pass a permission name to the Activate Session-Based Permission Set action. First, add a record lookup element to your flow to look up the PermissionSet object. Set the Name field to the name of your session-based permission set. Then add the Activate Session-Based Permission Set action, and set the input to your permission set name.

Tip: Make sure that users who want to run your flow have the Run Flows permission.

When the flow activates the session-based permission set, the running user obtains access to the permissions specified in your permission set during the current user session. If the flow deactivates the session-based permission set, the permissions are no longer available to the user.

SEE ALSO:

Permission Sets

What Are Session-Based Permission Sets?

Flow Activate Session-Based Permission Set Element

Permission Sets Considerations

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Be aware of these considerations and special behaviors for permission sets.

Differences between new and cloned permission sets

A new permission set starts with no user license selected and no permissions enabled. A cloned permission set has the same user license and enabled permissions as the permission set that it's cloned from. You can't change the user license in a cloned permission set. Clone a permission set only if the new one requires the same user license as the original.

Limits

Make sure to refer to the Salesforce Features and Editions Limits for your specific edition.

User license restrictions

Some user licenses restrict the number of custom apps or tabs that a user can access. In this case, you can assign only the allotted number through the user's assigned profile and permission sets. For example, a user with the Force.com App Subscription user license with access to one Force.com Light App can access only that app's custom tabs.

Assigned apps

Assigned app settings specify the apps that users can select in the Force.com app menu. Unlike profiles, you can't assign a default app in permission sets. You can only specify whether apps are visible.

Permission sets and profiles

In API version 25.0 and later, every profile is automatically associated with a permission set, whether you explicitly assign it to one or not. This permission set stores the profile's user, object, and field permissions, plus setup entity access settings. You can query on these profile-owned permission sets but not modify them. They're not visible in the user interface.

Permission sets and permission set licenses

In API version 38.0 and later, you can create a permission set and associate it with a permission set license. When you create a permission set using a specific permission set license, users assigned to the permission set receive all functionality associated with the permission set license.

Apex class access

You can specify which methods in a top-level Apex class are executable for a permission set. Apex class access settings apply only to:

- Apex class methods, such as Web service methods
- Any method used in a custom Visualforce controller or controller extension applied to a Visualforce page

Triggers always fire on trigger events (such as `insert` or `update`), regardless of permission settings.

SEE ALSO:

How is record type access specified?

Object Permissions

Salesforce Features and Edition Limits

Assign a Feature Permission Set License and Permission Set

Make sure to follow instructions for your permission set license-related feature. You can't add permission sets that are associated with permission set licenses to managed packages.

Note: If you purchased a license that comes with standard permission sets, such as Sales Console User, permission sets are auto-generated for you.

1. From Setup, enter *`Company Information`* in the `Quick Find` box, then select **Company Information** and scroll down to Permission Set Licenses.
   You can see how many permission set licenses are available and have already been assigned. You can also see how many types of permission set licenses you have for different features.
2. From Setup, enter *`Permission Sets`* in the `Quick Find` box, then select **Permission Sets**.
3. Click **New**.
4. Enter your permission set information.
5. For License, select the license to associate with this permission set.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

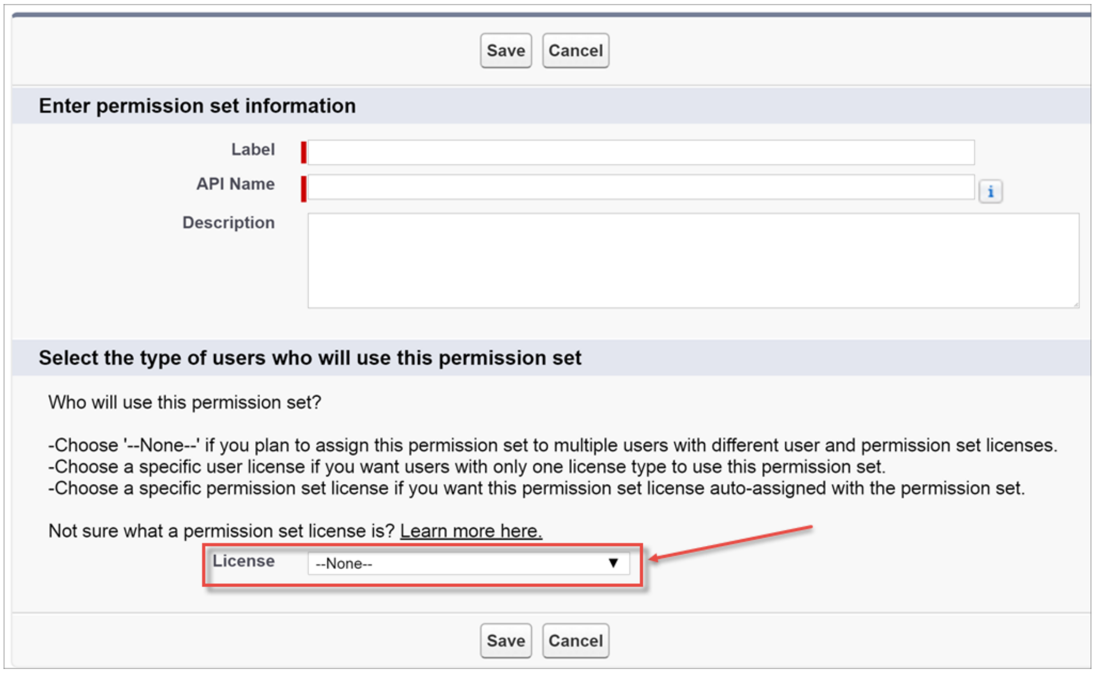
USER PERMISSIONS

To assign a permission set license:

- Manage Users

To assign a permission set to users:

- Assign Permission Sets



Enter permission set information

Label

API Name

Description

Select the type of users who will use this permission set

Who will use this permission set?

-Choose '--None--' if you plan to assign this permission set to multiple users with different user and permission set licenses.
-Choose a specific user license if you want users with only one license type to use this permission set.
-Choose a specific permission set license if you want this permission set license auto-assigned with the permission set.

Not sure what a permission set license is? Learn more here.

License --None--

When you select a specific permission set license, any user assigned to the permission set is *auto-assigned* the permission set license. If you select --None--, you must *manually* assign the permission set license to users before you can add them to the new permission set.

6. Select the feature permissions to enable for your permission set. Use `Find Settings` to search for them quickly. Refer to the documentation for your feature to see which permissions are available with a specific permission set license.

Example: Let's say you purchased an Identity Connect permission set license. This permission set license contains a permission that grants access to the Identity Connect product features, such as providing Active Directory integration. To grant a user access to this permission:

- Ensure that the user has the Identity Connect permission set license. Users who don't have the associated permission set license for a permission set you create can't use the permission set. You can check which permission set licenses a user has by viewing the Permission Set License Assignments section of the user detail page.
- Create a permission set and name it something like "Identity Connect Permissions." From License, choose **Identity Connect**. While still in the permission set, go to `Find Settings`, search for **Identity Connect**, and select the **Use Identity Connect** system permission.
- Assign a user to the permission set.

Permission Set Overview Page

A permission set's overview page provides an entry point for all of the permissions in a permission set. To open a permission set overview page, from Setup, enter `Permission Sets` in the `Quick Find` box, then select **Permission Sets** and select the permission set you want to view.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To delete permission sets and edit permission set properties:

- Manage Profiles and Permission Sets

App and System Settings in Permission Sets

In permission sets, permissions and settings are organized into app and system categories. These categories reflect the rights users need to administer and use system and app resources.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

App Settings

Apps are sets of tabs that users can change by selecting the drop-down menu in the header. All underlying objects, components, data, and configurations remain the same, regardless of the selected app. In selecting an app, users navigate in a set of tabs that allows them to efficiently use the underlying functionality for app-specific tasks. For example, let's say you do most of your work in the sales app, which includes tabs like Accounts and Opportunities. To track a new marketing campaign, rather than adding the Campaigns tab to the sales app, you select Marketing from the app drop-down to view your campaigns and campaign members.

The Apps section of the permission sets overview page contains settings that are directly associated with the business processes the apps enable. For example, customer service agents might need to manage cases, so the “Manage Cases” permission is in the Call Center section of the App Permissions page. Some app settings aren't related to app permissions. For example, to enable the Time-Off Manager app from the AppExchange, users need access to the appropriate Apex classes and Visualforce pages, as well as the object and field permissions that allow them to create new time-off requests.

System Settings

Some system functions apply to an organization and not to any single app. For example, “View Setup and Configuration” allows users to view setup and administrative settings pages. Other system functions apply to all apps. For example, the “Run Reports” and “Manage Dashboards” permissions allow managers to create and manage reports in all apps. In some cases, such as with “Modify All Data,” a permission applies to all apps, but also includes non-app functions, like the ability to download the Data Loader.

IN THIS SECTION:

- Work with Assigned Apps in Permission Sets
- Working with Object Settings in Permission Sets
- App Permissions in Permission Sets
- Working with Visualforce Page Access in Permission Sets
- Working with System Permissions in Permission Sets
- Working with Service Provider Access in Permission Sets

SEE ALSO:

- Permission Sets
- What Are Permission Set Licenses?

Search Permission Sets

To quickly navigate to other pages in a permission set, you can enter search terms in any permission set detail page.

On any of the permission sets detail pages, type at least three consecutive letters of an object, setting, or permission name in the **Find Settings...** box. The search terms aren't case-sensitive. As you type, suggestions for results that match your search terms appear in a list. Click an item in the list to go to its settings page.

For some categories, you can search for the specific permission or setting name. For other categories, search for the category name.

Item	Search for	Example
Assigned apps	App name	Type `sales` in the Find Settings box, then select `Sales` from the list.
Objects	Object name	Let's say you have an Albums custom object. Type `albu`, then select `Albums`.
• Fields • Record types	Parent object name	Let's say your Albums object contains a Description field. To find the `Description` field for albums, type `albu`, select `Albums`, and scroll down to `Description` under Field Permissions.
Tabs	Tab or parent object name	Type `rep`, then select `Reports`.
App and system permissions	Permission name	Type `api`, then select `API Enabled`.
All other categories	Category name	To find Apex class access settings, type `apex`, then select `Apex Class Access`. To find custom permissions, type `cust`, then select `Custom Permissions`. And so on.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To search permission sets:

- View Setup and Configuration

If you don't get any results, don't worry. Here's some tips that can help:

- Check if the search term has at least three consecutive characters that match the object, setting, or permission name.
- The permission, object, or setting you're searching for might not be available in the current Salesforce org.
- The item you're searching for might not be available for the user license that's associated with the current permission set. For example, a permission set with the Standard Platform User license doesn't include the "Modify All Data" permission.
- The permission set license associated with the permission set doesn't include the object, setting, or permission name you're searching for.

SEE ALSO:

Permission Sets

View and Edit Assigned Apps in Permission Sets

Assigned app settings specify the apps that users can select in the Force.com app menu.

Unlike profiles, you can't assign a default app in permission sets. You can only specify whether apps are visible.

To assign apps:

1. From Setup, enter *`Permission Sets`* in the `Quick Find` box, then select **Permission Sets**.
2. Select a permission set, or create one.
3. On the permission set overview page, click **Assigned Apps**.
4. Click **Edit**.
5. To assign apps, select them from the Available Apps list and click **Add**. To remove apps from the permission set, select them from the Enabled Apps list and click **Remove**.
6. Click **Save**.

SEE ALSO:

Permission Sets

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit assigned app settings:

- Manage Profiles and Permission Sets

Assign Custom Record Types in Permission Sets

1. From Setup, enter `Permission Sets` in the `Quick Find` box, then select **Permission Sets**.
2. Select a permission set, or create one.
3. On the permission set overview page, click **Object Settings**, then click the object you want.
4. Click **Edit**.
5. Select the record types you want to assign to this permission set.
6. Click **Save**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Record types available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To assign record types in permission sets:

- Manage Profiles and Permission Sets

IN THIS SECTION:

How is record type access specified?

You can assign record types to users in their profile or permission sets, or a combination of both. Record type assignment behaves differently in profiles and permission sets.

SEE ALSO:

How is record type access specified?

How is record type access specified?

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

You can assign record types to users in their profile or permission sets, or a combination of both. Record type assignment behaves differently in profiles and permission sets.

- A user's default record type is specified in the user's personal settings. You can't specify a default record type in permission sets.
- You can assign the `--Master--` record type in profiles. In permission sets, you can assign only custom record types. The behavior for record creation depends on which record types are assigned in profiles and permission sets.

If users have this record type on their profile...	And this total number of custom record types in their permission sets...	When they create a record...
`--Master--`	None	The new record is associated with the Master record type
`--Master--`	One	The new record is associated with the custom record type. Users can't select the Master record type.
`--Master--`	Multiple	Users are prompted to select a record type.
Custom	One or more	Users are prompted to select a record type. In their personal settings, users can set an option to use their default

If users have this record type on their profile...	And this total number of custom record types in their permission sets...	When they create a record...
		record type and not be prompted to choose a record type.

- Page layout assignments are specified in profiles only—they're not available in permission sets. When a permission set specifies a custom record type, users with that permission set get the page layout assignment that's specified for that record type in their profile. (In profiles, page layout assignments are specified for every record type, even when record types aren't assigned.)
- For lead conversion, the default record type specified in a user's profile is used for the converted records.
- Users can view records assigned to any record type. As a result, a page layout is assigned to every record type on a user's profile. A record type assignment on a user's profile or permission set doesn't determine whether a user can view a record with that record type. The record type assignment simply specifies that the user can use that record type when creating or editing a record.
- Record types in permission sets aren't supported in packages and change sets. As a result, any record type assignments in permission sets in a sandbox organization must be manually reproduced in a production organization.

SEE ALSO:

Assign Record Types and Page Layouts in the Enhanced Profile User Interface

Assign Record Types to Profiles in the Original Profile User Interface

Assign Custom Record Types in Permission Sets

Assign Page Layouts in the Original Profile User Interface

Enable Custom Permissions in Permission Sets

Custom permissions give you a way to provide access to custom processes or apps. After you've created a custom permission and associated it with a process or app, you can enable the permission in permission sets.

1. From Setup, enter `Permission Sets` in the `Quick Find` box, then select **Permission Sets**.
2. Select a permission set, or create one.
3. On the permission set overview page, click **Custom Permissions**.
4. Click **Edit**.
5. To enable custom permissions, select them from the Available Custom Permissions list and then click **Add**. To remove custom permissions from the permission set, select them from the Enabled Custom Permissions list and then click **Remove**.
6. Click **Save**.

SEE ALSO:

Custom Permissions

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

In Group and Professional Edition organizations, you can't create or edit custom permissions, but you can install them as part of a managed package.

USER PERMISSIONS

To enable custom permissions in permission sets:

- Manage Profiles and Permission Sets

Manage Permission Set Assignments

You can assign permission sets to a single user from the user detail page or assign multiple users to a permission set from any permission set page.

- Assign Permission Sets to a Single User
- Assign a Permission Set to Multiple Users
- Remove User Assignments from a Permission Set

IN THIS SECTION:

Permission Set Assigned Users Page
From the Assigned Users page, you can view all users who are assigned to a permission set, assign more users, and remove user assignments.

Assign Permission Sets to a Single User
Assign permission sets or remove permission set assignments for a single user from the user detail page.

Assign a Permission Set to Multiple Users
Assign a permission set to one or more users from any permission set page.

Remove User Assignments from a Permission Set
From any permission set page, you can remove the permission set assignment from one or more users.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Permission Set Assignment Summary Page

Permission Set Assigned Users Page

From the Assigned Users page, you can view all users who are assigned to a permission set, assign more users, and remove user assignments.

To view all users who are assigned to a permission set, from any permission set page, click **Manage Assignments**. From the Assigned Users page, you can:

- Assign users to the permission set
- Remove user assignments from the permission set
- Edit a user
- View a user's detail page by clicking the name, alias, or username
- View a profile by clicking the profile name

SEE ALSO:

Assign Permission Sets to a Single User

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view users that are assigned to a permission set:

- View Setup and Configuration

Assign Permission Sets to a Single User

Assign permission sets or remove permission set assignments for a single user from the user detail page.

The Permission Set Assignments page shows:

- Permission sets with no associated license. For example, you can assign a permission set if **None** was selected for the license type in the permission set. Make sure that the user's license allows all the permission set's enabled settings and permissions. If the user's license doesn't allow selected permissions, the assignment fails.
- Permission sets that match the user's license. For example, if a user's license is Chatter Only, you can assign permission sets with the Chatter Only license.
- Permission sets specific to permission set licenses. Let's say you create a permission set named Identity and associate that permission set to the "Identity Connect" permission set license. When you assign users to Identity, they receive all functionality available with the Identity Connect permission set license.

Note: Some permissions require users to have a permission set license before you can grant the permissions. For example, if you add the "Use Identity Connect" user permission to the Identity permission set, you can assign only users with the Identity Connect permission set license to the permission set.

1. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.
2. Select a user.
3. In the Permission Set Assignments related list, click **Edit Assignments**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To assign permission sets:

- "Assign Permission Sets"

4. To assign a permission set, select it under Available Permission Sets and click **Add**. To remove a permission set assignment, select it under Enabled Permission Sets and click **Remove**.
5. Click **Save**.

Tip: You can perform this and other administration tasks from the SalesforceA mobile app.

SEE ALSO:

Assign a Permission Set to Multiple Users

Standard Permission Sets

Help Users From Anywhere With SalesforceA

Assign a Permission Set to Multiple Users

Assign a Permission Set to Multiple Users

Assign a permission set to one or more users from any permission set page.

1. Select the permission set that you want to assign to users.
2. Click **Manage Assignments** and then **Add Assignments**.
3. Select the checkboxes next to the names of the users you want assigned to the permission set, and click **Assign**.

Messages confirm success or indicate if a user doesn't have the appropriate licenses for assignment.

SEE ALSO:

Remove User Assignments from a Permission Set

Assign Permission Sets to a Single User

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To assign a permission set to users:

- Assign Permission Sets

Remove User Assignments from a Permission Set

From any permission set page, you can remove the permission set assignment from one or more users.

1. From Setup, enter `Permission Sets` in the `Quick Find` box, then select **Permission Sets**.
2. Select a permission set.
3. In the permission set toolbar, click **Manage Assignments**.
4. Select the users to remove from this permission set.

   You can remove up to 1000 users at a time.
5. Click **Remove Assignments**.

   This button is only available when one or more users are selected.
6. To return to a list of all users assigned to the permission set, click **Done**.

SEE ALSO:

Assign a Permission Set to Multiple Users

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To remove permission set assignments:
- Assign Permission Sets

Revoking Permissions and Access

You can use profiles and permission sets to grant access, but not to deny access. Any permission granted from either a profile or permission set is honored. For example, if "Transfer Record" isn't enabled in Jane Smith's profile, but is enabled in two of her permission sets, she can transfer records regardless of whether she owns them. To revoke a permission, you must remove all instances of the permission from the user. You can do this with the following actions—each has possible consequences.

Action	Consequence
Disable a permission or remove an access setting in the profile and any permission sets that are assigned to the user.	The permission or access setting is disabled for all other users assigned to the profile or permission sets.
If a permission or access setting is enabled in the user's profile, assign a different profile to the user. AND If the permission or access setting is enabled in any permission sets that are assigned to the user, remove the permission set assignments from the user.	The user may lose other permissions or access settings associated with the profile or permission sets.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

To resolve the consequence in either case, consider all possible options. For example, you can clone the assigned profile or any assigned permission sets where the permission or access setting is enabled. Then, disable the permission or access setting, and assign the cloned profile or permission sets to the user. Another option is to create a base profile with the least number of permissions and settings that represents the largest number of users possible. Then create permission sets that layer more access.

SEE ALSO:

User Permissions and Access

Assign Permission Sets to a Single User

What Determines Field Access?

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Page layouts are not available in **Database.com**

Several factors control whether users can view and edit specific fields in Salesforce. You can control users' access to fields at the record type, user, or field level.

- **Page layouts**—Set whether fields are visible, required, editable, or read only for a particular record type.
- **Field-level security**—Further restrict users' access to fields by setting whether those fields are visible, editable, or read only. These settings override field properties set in the page layout if the field-level security setting is more restrictive.
- **Permissions**—Some user permissions override both page layouts and field-level security settings. For example, users with the "Edit Read Only Fields" permission can always edit read-only fields regardless of any other settings.
- **Universally required fields**—Override field-level security or any less-restrictive settings on page layouts by making a custom field universally required.

After setting these items, confirm users' access to specific fields using the field accessibility grid.

SEE ALSO:

Modifying Field Access Settings

Verify Access for a Particular Field

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view field accessibility:

- View Setup and Configuration

See whether access to a field is restricted and at what level—record type, user profile, or field.

1. Navigate to the fields area of the appropriate object:
   - For Knowledge validation status picklists, from Setup, enter *`Validation Statuses`* in the `Quick Find` box, then select **Validation Statuses**.
2. Select a field and click **View Field Accessibility**.
3. Confirm that the field access is correct for different profiles and record types.
4. Hover over any field access setting to see whether the field is required, editable, hidden, or read only based on the page layout or field-level security.
5. Click any field access setting to change it.

To verify field accessibility by a specific profile, record type, or field, from Setup, enter *`Field Accessibility`* in the `Quick Find` box, then select **Field Accessibility**. From this page, choose a particular tab to view and then select whether you want to check access by profiles, record types, or fields.

Note: In this user interface, you can't check access for permission sets.

SEE ALSO:

What Determines Field Access?

Modifying Field Access Settings

From the field accessibility grid, you can click any field access setting to change the field's accessibility in the page layout or in field-level security. The Access Settings page then lets you modify the field access settings.

- In the Field-Level Security section of the page, specify the field's access level for the profile.

Access Level	Enabled Settings
Users can read and edit the field.	**Visible**
Users can read but not edit the field.	**Visible** and **Read-Only**
Users can't read or edit the field.	None

  We recommend that you use field-level security to control users' access to fields rather than creating multiple page layouts to control field access.

- In the Page Layout section of the page, you can:
  - Select the `Remove or change editability` radio button and then change the field access properties for the page layout. These changes will affect all profile and record type combinations that currently use this page layout.
  - Alternatively, you can select the `Choose a different page layout` radio button to assign a different page layout to the profile and record type combination.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view field accessibility:
- View Setup and Configuration

To change field accessibility:
- Customize Application

  AND

  Manage Profiles and Permission Sets

SEE ALSO:

What Determines Field Access?

Field-Level Security

Field-level security settings let you restrict users' access to view and edit specific fields.

Note: Who Sees What: Field-Level Security (English only)

Watch how you can restrict access to specific fields on a profile-by-profile basis.

Your Salesforce org contains a lot of data, but you probably don't want every field accessible to everyone. For example, your payroll manager probably wants to keep salary fields accessible only to select employees. You can restrict user access in:

- Detail and edit pages
- Related lists

EDITIONS

Available in: Salesforce Classic

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

- List views
- Reports
- Connect Offline
- Email and mail merge templates
- Custom links
- The partner portal
- The Salesforce Customer Portal
- Synchronized data
- Imported data

The fields that users see on detail and edit pages are a combination of page layouts and field-level security settings. The most restrictive field access settings of the two always applies. For example, you can have a field that's required in a page layout but is read-only in the field-level security settings. The field-level security overrides the page layout, so the field remains read-only.

> Important: Field-level security doesn't prevent searching on the values in a field. When search terms match on field values protected by field-level security, the associated records are returned in the search results without the protected fields and their values.

You can define field-level security in either of these ways.

- For multiple fields on a single permission set or profile
- For a single field on all profiles

After setting field-level security, you can:

- Create page layouts to organize the fields on detail and edit pages.

  > Tip: Use field-level security to restrict users' access to fields, and then use page layouts to organize detail and edit pages within tabs. This approach reduces the number of page layouts for you to maintain.

- Verify users' access to fields by checking field accessibility.
- Customize search layouts to set the fields that appear in search results, in lookup dialog search results, and in the key lists on tab home pages.

> Note: Roll-up summary and formula fields are read-only on detail pages and not available on edit pages. They can also be visible to users even though they reference fields that your users can't see. Universally required fields appear on edit pages regardless of field-level security.
>
> The relationship group wizard allows you to create and edit relationship groups regardless of field-level security.

Set Field Permissions in Permission Sets and Profiles

Field permissions specify the access level for each field in an object.

1. From Setup, either:
   - Enter *`Permission Sets`* in the `Quick Find` box, then select **Permission Sets**, or
   - Enter *`Profiles`* in the `Quick Find` box, then select **Profiles**
2. Select a permission set or profile.
3. Depending on which interface you're using, do one of the following:
   - Permission sets or enhanced profile user interface—In the **Find Settings...** box, enter the name of the object you want and select it from the list. Click **Edit**, then scroll to the Field Permissions section.
   - Original profile user interface—In the Field-Level Security section, click **View** next to the object you want to modify, and then click **Edit**.
4. Specify the field's access level.
5. Click **Save**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To set field-level security:

- Manage Profiles and Permission Sets

  AND

  Customize Application

Set Field-Level Security for a Single Field on All Profiles

1. From the management settings for the field's object, go to the fields area.
2. Select the field you want to modify.
3. Click **View Field Accessibility**.
4. Specify the field's access level.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To set field-level security:

- Manage Profiles and Permission Sets

  AND

  Customize Application

User Permissions

User permissions specify what tasks users can perform and what features users can access. For example, users with the "View Setup and Configuration" permission can view Setup pages, and users with the "API Enabled" permission can access any Salesforce API.

You can enable user permissions in permission sets and custom profiles. In permission sets and the enhanced profile user interface, these permissions—as well as their descriptions—are listed in the App Permissions or System Permissions pages. In the original profile user interface, user permissions are listed under Administrative Permissions and General User Permissions.

To view permissions and their descriptions, from Setup, enter *Permission Sets* in the `Quick Find` box, then select **Permission Sets**, then select or create a permission set. Then from the Permission Set Overview page, click **App Permissions** or **System Permissions**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

The user permissions available vary according to which edition you have.

SEE ALSO:

- Profiles
- Permission Sets
- Standard Profiles

Object Permissions

Object permissions specify the base-level access users have to create, read, edit, and delete records for each object. You can manage object permissions in permission sets and profiles.

Object permissions either respect or override sharing rules and settings. The following permissions specify the access that users have to objects.

Permission	Description	Respects or Overrides Sharing?
Read	Users can only view records of this type.	Respects sharing
Create	Users can read and create records.	Respects sharing
Edit	Users can read and update records.	Respects sharing
Delete	Users can read, edit, and delete records.	Respects sharing
View All	Users can view all records associated with this object, regardless of sharing settings.	Overrides sharing

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Permission	Description	Respects or Overrides Sharing?
Modify All	Users can read, edit, delete, transfer, and approve all records associated with this object, regardless of sharing settings. Note: "Modify All" on documents allows access to all shared and public folders, but not the ability to edit folder properties or create new folders. To edit folder properties and create new folders, users must have the "Manage Public Documents" permission.	Overrides sharing

SEE ALSO:

- "View All" and "Modify All" Permissions Overview
- Comparing Security Models
- Field Permissions

"View All" and "Modify All" Permissions Overview

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in all editions

The "View All" and "Modify All" permissions ignore sharing rules and settings, allowing administrators to grant access to records associated with a given object across the organization. "View All" and "Modify All" can be better alternatives to the "View All Data" and "Modify All Data" permissions.

Be aware of the following distinctions between the permission types.

Permissions	Used for	Users who need them
View All Modify All	Delegation of object permissions.	Delegated administrators who manage records for specific objects
View All Data Modify All Data	Managing all data in an organization; for example, data cleansing, deduplication, mass deletion, mass transferring, and managing record approvals. Users with View All Data (or Modify All Data) permission can view (or modify) all apps and data, even if the apps and data are not shared with them.	Administrators of an entire organization
View All Users	Viewing all users in the organization. Grants Read access to all users, so that you can see their user record details, see them in searches, list views, and so on.	Users who need to see all users in the organization. Useful if the organization-wide default for the user object is Private. Administrators with the "Manage Users" permission are automatically granted the "View All Users" permission.

“View All” and “Modify All” are not available for ideas, price books, article types, and products.

“View All” and “Modify All” allow for delegation of object permissions only. To delegate user administration and custom object administration duties, define delegated administrators.

“View All Users” is available if your organization has User Sharing, which controls user visibility in the organization. To learn about User Sharing, see User Sharing.

SEE ALSO:

Object Permissions

Comparing Security Models

EDITIONS

Available in: Salesforce Classic

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

Salesforce user security is an intersection of sharing, and user and object permissions. In some cases, such as in end-user record level access, it is advantageous to use sharing to provide access to records. In other cases, such as when delegating record administration tasks like transferring records, cleansing data, deduplicating records, mass deleting records, and delegating workflow approval processes, it is advantageous to override sharing and use permissions to provide access to records.

The “Read,” “Create,” “Edit,” and “Delete” permissions respect sharing settings, which control access to data at the record level. The “View All” and “Modify All” permissions override sharing settings for specific objects. Additionally, the “View All Data” and “Modify All Data” permissions override sharing settings for *all* objects.

The following table describes the differences between the security models.

	Permissions that Respect Sharing	Permissions that Override Sharing
Target audience	End-users	Delegated data administrators
Where managed	“Read,” “Create,” “Edit,” and “Delete” object permissions; Sharing settings	“View All” and “Modify All”
Record access levels	Private, Read-Only, Read/Write, Read/Write/Transfer/Full Access	“View All” and “Modify All”
Ability to transfer	Respects sharing settings, which vary by object	Available on all objects with “Modify All”
Ability to approve records, or edit and unlock records in an approval process	None	Available on all objects with “Modify All”
Ability to report on all records	Available with a sharing rule that states: the records owned by the public group “Entire Organization” are shared with a specified group, with Read-Only access	Available on all objects with “View All”
Object support	Available on all objects except products, documents, solutions, ideas, notes, and attachments	Available on most objects via object permissions Note: “View All” and “Modify All” are not available for ideas, price books, article types, and products.

	Permissions that Respect Sharing	Permissions that Override Sharing
Group access levels determined by	Roles, Roles and Subordinates, Roles and Internal Subordinates, Roles, Internal and Portal Subordinates, Queues, Teams, and Public Groups	Profile or permission sets
Private record access	Not available	Available on private contacts, opportunities, and notes and attachments with "View All" and "Modify All"
Ability to manually share records	Available to the record owner and any user above the record owner in the role hierarchy	Available on all objects with "Modify All"
Ability to manage all case comments	Not available	Available with "Modify All" on cases

Field Permissions

Field permissions specify the access level for each field in an object. In permission sets and the enhanced profile user interface, the setting labels differ from those in the original profile user interface and in field-level security pages for customizing fields.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Access Level	Enabled Settings in Permission Sets and Enhanced Profile User Interface	Enabled Settings in Original Profile and Field-Level Security Interfaces
Users can read and edit the field.	`Read` and `Edit`	`Visible`
Users can read but not edit the field.	`Read`	`Visible` and `Read-Only`
Users can't read or edit the field.	None	None

SEE ALSO:

Field-Level Security

Object Permissions

Sharing Settings

In Salesforce, you can control access to data at many different levels. For example, you can control the access your users have to objects with object permissions. Within objects, you can control the access users have to fields using field-level security. To control access to data at the record level, use sharing settings.

Note: Who Sees What: Overview (English only)

Watch how you can control who sees what data in your organization.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Teams are not available in **Database.com**

Organization-Wide Defaults

Your organization-wide default sharing settings give you a baseline level of access for each object and enable you to extend that level of access using hierarchies or sharing rules. For example, you can set the organization-wide default for leads to Private if you only want users to view and edit the leads they own. Then, you can create lead sharing rules to extend access of leads to particular users or groups.

Sharing Rules

Sharing rules represent the exceptions to your organization-wide default settings. If you have organization-wide sharing defaults of Public Read Only or Private, you can define rules that give additional users access to records they do not own. You can create sharing rules based on record owner or field values in the record.

Tip: Sometimes it's impossible to define a consistent group of users who need access to a particular set of records. In those situations, record owners can use manual sharing to give read and edit permissions to users who would not have access to the record any other way. Although manual sharing isn't automated like organization-wide sharing settings, role hierarchies, or sharing rules, it gives record owners the flexibility to share particular records with users that need to see them.

Apex Managed Sharing

Apex managed sharing allows developers to programmatically share custom objects. When you use Apex managed sharing to share a custom object, only users with the "Modify All Data" permission can add or change the sharing on the custom object's record, and the sharing access is maintained across record owner changes.

Other Methods for Allowing Access to Records

In addition to sharing settings, there are a few other ways to allow multiple users access to given records:

Map category groups to roles

Control access to data categories by mapping them to user roles.

Queues

Queues help you prioritize, distribute, and assign records to teams who share workloads. Queue members and users higher in a role hierarchy can access queues from list views and take ownership of records in a queue.

Use queues to route lead, order, case, and custom object records to a group.

Teams

For accounts, opportunities, and cases, record owners can use teams to allow other users access to their records. A *team* is a group of users that work together on an account, sales opportunity, or case. Record owners can build a team for each record that they own. The record owner adds team members and specifies the level of access each team member has to the record, so that some team members can have read-only access and others can have read/write access. The record owner can also specify a role for each team member, such as "Executive Sponsor." In account teams, team members also have access to any contacts, opportunities, and cases associated with an account.

Note: A team member may have a higher level of access to a record for other reasons, such as a role or sharing rule. In this case, the team member has the highest access level granted, regardless of the access level specified in the team.

SEE ALSO:

Organization-Wide Sharing Defaults

Sharing Rules

User Role Hierarchy

Sharing Considerations

Organization-Wide Sharing Defaults

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Customer Portal is not available in **Database.com**

Administrators can use organization-wide sharing settings to define the default sharing settings for an organization.

Organization-wide sharing settings specify the default level of access to records and can be set separately for accounts (including contracts), activities, assets, contacts, campaigns, cases, leads, opportunities, calendars, price books, orders, and custom objects.

For most objects, organization-wide sharing settings can be set to Private, Public Read Only, or Public Read/Write. In environments where the organization-wide sharing setting for an object is Private or Public Read Only, an administrator can grant users additional access to records by setting up a role hierarchy or defining sharing rules. However, sharing rules can only be used to grant additional access—they cannot be used to restrict access to records beyond what was originally specified with the organization-wide sharing defaults.

Important: If your organization uses a Customer Portal, before you enable contacts to access the portal, set the organization-wide sharing defaults on accounts, contacts, contracts, assets, and cases to Private. This ensures that by default your customers can view only their own data. You can still grant your Salesforce users Public Read/Write access by creating sharing rules in which all internal users share with all internal users.

By default, Salesforce uses hierarchies, like the role or territory hierarchy, to automatically grant access of records to users above the record owner in the hierarchy.

Setting an object to Private makes those records visible only to record owners and those above them in the role hierarchy. Use the **Grant Access Using Hierarchies** checkbox to disable access to records to users above the record owner in the hierarchy for custom objects in Professional, Enterprise, Unlimited, Performance, and Developer Edition. If you deselect this checkbox for a custom object, only the record owner and users granted access by the organization-wide defaults receive access to the records.

SEE ALSO:

Set Your Organization-Wide Sharing Defaults

Sharing Default Access Settings

Default Organization-Wide Sharing Settings

Set Your Organization-Wide Sharing Defaults

Organization-wide sharing defaults set the baseline access for your records. You can set the defaults separately for different objects.

Note: ▶ Who Sees What: Organization-Wide Defaults (English only)

Watch how you can restrict access to records owned by other users.

1. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
2. Click **Edit** in the Organization-Wide Defaults area.
3. For each object, select the default access you want to use. If you have external organization-wide defaults, see External Organization-Wide Defaults Overview.
4. To disable automatic access using your hierarchies, deselect **Grant Access Using Hierarchies** for any custom object that does not have a default access of Controlled by Parent.

   Note: If **Grant Access Using Hierarchies** is deselected, users that are higher in the role or territory hierarchy don't receive automatic access. However, some users—such as those with the "View All" and "Modify All" object permissions and the "View All Data" and "Modify All Data" system permissions—can still access records they don't own.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To set default sharing access:

- Manage Sharing

When you update organization-wide defaults, sharing recalculation applies the access changes to your records. If you have a lot of data, the update can take longer.

- If you are increasing the default access, such as from Public Read Only to Public Read/Write, your changes take effect immediately. All users get access based on the updated default access. Sharing recalculation is then run asynchronously to ensure that all redundant access from manual or sharing rules are removed.

  Note: When the default access for contacts is Controlled by Parent and you increase the default access for accounts, opportunities, or cases, the changes take effect after recalculation is run.

- If you are decreasing the default access, such as from Public Read/Write to Public Read Only, your changes take effect after recalculation is run.

You'll receive a notification email when the recalculation completes. Refresh the Sharing Settings page to see your changes. To view the update status, from Setup, enter `View Setup Audit Trail` in the `Quick Find` box, then select **View Setup Audit Trail**.

Limitations

The organization-wide sharing default setting can't be changed for some objects:

- Service contracts are always Private.
- User provisioning requests are always Private.

- The ability to view or edit a document, report, or dashboard is based on a user's access to the folder in which it's stored.
- Users can only view the forecasts of other users who are placed below them in the role hierarchy, unless forecast sharing is enabled.
- When a custom object is on the detail side of a master-detail relationship with a standard object, its organization-wide default is set to Controlled by Parent and it is not editable.
- The organization-wide default settings can't be changed from private to public for a custom object if Apex code uses the sharing entries associated with that object. For example, if Apex code retrieves the users and groups who have sharing access on a custom object Invoice__c (represented as `Invoice__share` in the code), you can't change the object's organization-wide sharing setting from private to public.

SEE ALSO:

Sharing Default Access Settings

Organization-Wide Sharing Defaults

Sharing Default Access Settings

You can use organization-wide defaults to set the default level of record access for the following objects.

- Accounts and their associated contracts
- Activities
- Calendars
- Campaigns
- Cases
- Contacts
- Custom objects
- Leads
- Opportunities
- Orders
- Price books
- Service contracts
- Users

You can assign the following access levels to accounts, campaigns, cases, contacts, contracts, leads, opportunities, orders, users, and custom objects.

EDITIONS

Available in: Salesforce Classic

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

Only Custom Objects are available in **Database.com**

USER PERMISSIONS

To set default sharing access:

- Manage Sharing

Field	Description
`Controlled by Parent`	A user can perform an action (such as view, edit, or delete) on a contact or order based on whether he or she can perform that same action on the record associated with it. For example, if a contact is associated with the Acme account, then a user can only edit that contact if he or she can also edit the Acme account.

Field	Description
`Private`	Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records. For example, if Tom is the owner of an account, and he is assigned to the role of Western Sales, reporting to Carol (who is in the role of VP of Western Region Sales), then Carol can also view, edit, and report on Tom's accounts.
`Public Read Only`	All users can view and report on records but not edit them. Only the owner, and users above that role in the hierarchy, can edit those records. For example, Sara is the owner of ABC Corp. Sara is also in the role Western Sales, reporting to Carol, who is in the role of VP of Western Region Sales. Sara and Carol have full read/write access to ABC Corp. Tom (another Western Sales Rep) can also view and report on ABC Corp, but cannot edit it.
`Public Read/Write`	All users can view, edit, and report on all records. For example, if Tom is the owner of Trident Inc., all other users can view, edit, and report on the Trident account. However, only Tom can alter the sharing settings or delete the Trident account.
`Public Read/Write/Transfer`	All users can view, edit, transfer, and report on all records. Only available for cases or leads. For example, if Alice is the owner of ACME case number 100, all other users can view, edit, transfer ownership, and report on that case. But only Alice can delete or change the sharing on case 100.
`Public Full Access`	All users can view, edit, transfer, delete, and report on all records. Only available for campaigns. For example, if Ben is the owner of a campaign, all other users can view, edit, transfer, or delete that campaign.

Note: To use cases effectively, set the organization-wide default for Account, Contact, Contract, and Asset to Public Read/Write.

You can assign the following access levels to personal calendars.

Field	Description
`Hide Details`	Others can see whether the user is available at given times, but can not see any other information about the nature of events in the user's calendar.
`Hide Details and Add Events`	In addition to the sharing levels set by Hide Details, users can insert events in other users' calendars.

Field	Description
`Show Details`	Users can see detailed information about events in other users' calendars.
`Show Details and Add Events`	In addition to the sharing levels set by Show Details, users can insert events in other users' calendars.
`Full Access`	Users can see detailed information about events in other users' calendars, insert events in other users' calendars, and edit existing events in other users' calendars.

Note: Regardless of the organization-wide defaults that have been set for calendars, all users can invite all other users to events.

You can assign the following access levels to price books.

Field	Description
`Use`	All users can view price books and add them to opportunities. Users can add any product within that price book to an opportunity.
`View Only`	All users can view and report on price books but only users with the "Edit" permission on opportunities or users that have been manually granted use access to the price book can add them to opportunities.
`No Access`	Users cannot see price books or add them to opportunities. Use this access level in your organization-wide default if you want only selected users to access selected price books. Then, manually share the appropriate price books with the appropriate users.

You can assign the following access levels to activities.

Field	Description
`Private`	Only the activity owner, and users above the activity owner in the role hierarchy, can edit and delete the activity; users with read access to the record to which the activity is associated can view and report on the activity.
`Controlled by Parent`	A user can perform an action (such as view, edit, transfer, and delete) on an activity based on whether he or she can perform that same action on the records associated with the activity. For example, if a task is associated with the Acme account and the John Smith contact, then a user can only edit that task if he or she can also edit the Acme account and the John Smith record.

You can assign the following access levels to users.

Field	Description
`Private`	All users have read access to their own user record and those below them in the role hierarchy.
`Public Read Only`	All users have read access on one another. You can see all users' detail pages. You can also see all users in lookups, list views, ownership changes, user operations, and search.

SEE ALSO:

Set Your Organization-Wide Sharing Defaults

Default Organization-Wide Sharing Settings

EDITIONS

Accounts, cases, contacts, leads, opportunities, and custom objects available in: Salesforce Classic and Lightning Experience

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

Except for Custom Objects, all object types are not available in **Database.com**

The default organization-wide sharing settings are:

Object	Default Access
Account	Public Read/Write
Activity	Private
Asset	Controlled by Parent
Calendar	Hide Details and Add Events
Campaign	Public Full Access
Case	Public Read/Write/Transfer
Contact	Controlled by Parent
Contract	Public Read/Write
Custom Object	Public Read/Write
Lead	Public Read/Write/Transfer
Opportunity	Public Read Only
Price Book	Use
Service Contract	Private
Users	Public Read Only Private for external users

SEE ALSO:

Organization-Wide Sharing Defaults

Set Your Organization-Wide Sharing Defaults

External Organization-Wide Defaults Overview

EDITIONS

Available in: Salesforce Classic

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

External organization-wide defaults provide separate organization-wide defaults for internal and external users. They simplify your sharing rules configuration and improve recalculation performance. Additionally, administrators can easily see which information is being shared to portals and other external users.

The following objects support external organization-wide defaults.

- Accounts and their associated contracts and assets
- Cases
- Contacts
- Opportunities
- Custom Objects
- Users

External users include:

- Authenticated website users
- Chatter external users
- Community users
- Customer Portal users
- Guest users
- High-volume portal users
- Partner Portal users
- Service Cloud Portal users

Note: Chatter external users have access to the User object only.

Previously, if your organization wanted Public Read Only or Public Read/Write access for internal users but Private for external users, you would have to set the default access to Private and create a sharing rule to share records with all internal users.

With separate organization-wide defaults, you can achieve similar behavior by setting the default internal access to Public Read Only or Public Read/Write and the default external access to Private. These settings also speed up performance for reports, list views, searches, and API queries.

SEE ALSO:

Organization-Wide Sharing Defaults

Setting the External Organization-Wide Defaults

Sharing Default Access Settings

Setting the External Organization-Wide Defaults

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To set default sharing access:

- Manage Sharing

External Organization-Wide Defaults enable you to set a different default access level for external users.

Before you set the external organization-wide defaults, make sure that it is enabled. From Setup, enter *`Sharing Settings`* in the `Quick Find` box, then select **Sharing Settings**, and click the **Enable External Sharing Model** button.

When you first enable external organization-wide defaults, the default internal access and default external access are set to the original default access level. For example, if your organization-wide default for contacts is Private, the default internal access and default external access will be Private as well.

To set the external organization-wide default for an object:

1. From Setup, enter *`Sharing Settings`* in the `Quick Find` box, then select **Sharing Settings**
2. Click **Edit** in the Organization-Wide Defaults area.
3. For each object, select the default access you want to use.

   You can assign the following access levels.

Access Level	Description
`Controlled by Parent`	Users can perform actions (such as view, edit, delete) on a record on the detail side of a master-detail relationship if they can perform the same action on all associated master records. Note: For contacts, `Controlled by Parent` must be set for both the default internal and external access.
`Private`	Only users who are granted access by ownership, permissions, role hierarchy, manual sharing, or sharing rules can access the records.
`Public Read Only`	All users can view all records for the object.
`Public Read/Write`	All users can view and edit all records for the object.

   Note: The default external access level must be more restrictive or equal to the default internal access level. For example, you can have a custom object with default external access set to Private and default internal access set to Public Read Only.

4. Click **Save**.

SEE ALSO:

External Organization-Wide Defaults Overview

Disabling External Organization-Wide Defaults

Disabling External Organization-Wide Defaults results in one organization-wide default for each object.

Before disabling this feature, set **Default External Access** and **Default Internal Access** to the same access level for each object.

To disable the external organization-wide defaults:

1. From Setup, enter *`Sharing Settings`* in the `Quick Find` box, then select **Sharing Settings**
2. Click **Disable External Sharing Model** in the Organization-Wide Defaults area.

After disabling the external organization-wide defaults, you'll see the **Default Access** setting instead of the **Default External Access** and **Default Internal Access** settings in the organization-wide defaults area. If you have User Sharing, the **Default External Access** settings for the account, contact, case, and opportunity objects remain visible but they are disabled.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To disable external organization-wide defaults:

- Manage Sharing

SEE ALSO:

External Organization-Wide Defaults Overview

Controlling Access Using Hierarchies

Determine whether users have access to records they don't own, including records to which they don't have sharing access, but someone below them in the hierarchy does.

Beyond setting the organization-wide sharing defaults for each object, you can specify whether users have access to the data owned by or shared with their subordinates in the hierarchy. For example, the role hierarchy automatically grants record access to users above the record owner in the hierarchy. By default, the `Grant Access Using Hierarchies` option is enabled for all objects, and it can only be changed for custom objects.

To control sharing access using hierarchies for any custom object, from Setup, enter *`Sharing Settings`* in the `Quick Find` box, then select **Sharing Settings**. Next, click **Edit** in the Organization Wide Defaults section. Deselect `Grant Access Using Hierarchies` if you want to prevent users from gaining automatic access to data owned by or shared with their subordinates in the hierarchies.

EDITIONS

Available in: Salesforce Classic

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

Territories are not available in **Database.com**

USER PERMISSIONS

To set default sharing access and change the `Grant Access Using Hierarchies` option:

- Manage Sharing

Implementation Notes

- Regardless of your organization's sharing settings, users can gain access to records they do not own through other means such as user permissions like "View All Data," sharing rules, or manual sharing of individual records.
- The `Grant Access Using Hierarchies` option is always selected on standard objects and is not editable.
- If you disable the `Grant Access Using Hierarchies` option, sharing with a role or territory and subordinates only shares with the users directly associated with the role or territory selected. Users in roles or territories above them in the hierarchies will not gain access.
- If your organization disables the `Grant Access Using Hierarchies` option, activities associated with a custom object are still visible to users above the activity's assignee in the role hierarchy.

- If a master-detail relationship is broken by deleting the relationship, the former detail custom object's default setting is automatically reverted to Public Read/Write and `Grant Access Using Hierarchies` is selected by default.
- The `Grant Access Using Hierarchies` option affects which users gain access to data when something is shared with public groups, personal groups, queues, roles, or territories. For example, the **View All Users** option displays group members and people above them in the hierarchies when a record is shared with them using a sharing rule or manual sharing and the `Grant Access Using Hierarchies` option is selected. When the `Grant Access Using Hierarchies` option is not selected, some users in these groups no longer have access. The following list covers the access reasons that depend on the `Grant Access Using Hierarchies` option.

  These reasons always gain access:

  Group Member

  Queue Member

  Role Member

  Member of Subordinate Role

  Territory Member

  Member of Subordinate Territory

  These reasons only gain access when using hierarchies:

  Manager of Group Member

  Manager of Queue Member

  Manager of Role

  Manager of Territory

  User Role Manager of Territory

Best Practices

- When you deselect `Grant Access Using Hierarchies`, notify users of the changes in report results that they can expect due to losing visibility of their subordinates' data. For example, selecting My team's... in the View drop-down list returns records owned by the user; it will not include records owned by their subordinates. To be included in this type of report view, records from subordinates must be explicitly shared with that user by some other means such as a sharing rule or a manual share. So, if no records are shared with you manually, the My... and My team's... options in the View drop-down list return the same results. However, choosing the Activities with... any custom object report type when creating a custom report returns activities assigned to you as well as your subordinates in the role hierarchy.

SEE ALSO:

User Role Hierarchy

User Role Hierarchy

Salesforce offers a user role hierarchy that you can use with sharing settings to determine the levels of access that users have to your Salesforce org's data. Roles within the hierarchy affect access on key components such as records and reports.

> If your organization-wide defaults are more restrictive than Public Read/Write, use role hierarchy to make records more accessible to users.
>
> Watch a Demo: ▶ Who Sees What: Record Access via the Role Hierarchy (English only)

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create, edit, and delete roles:

- Manage Roles

To assign users to roles:

- Manage Internal Users

Users at any role level can view, edit, and report on all data that's owned by or shared with users below them in the role hierarchy, unless your Salesforce org's sharing model for an object specifies otherwise. Specifically, in the Organization-Wide Defaults related list, you can disable the **Grant Access Using Hierarchies** option for a custom object. When disabled, only the record owner and users who are granted access by the organization-wide defaults receive access to the object's records.

Roles determine user access to cases, contacts, and opportunities, regardless of who owns those records. The access level is specified on the Role Edit page. For example, you can set the contact access so that users in a role can edit all contacts associated with accounts that they own, regardless of who owns the contacts. And you can set the opportunity access so that users in a role can edit all opportunities associated with accounts that they own, regardless of who owns the opportunities.

After you share a folder with a role, it's visible only to users in that role, not to superior roles in the hierarchy.

Guidelines for Success with Roles

Understand key rule behaviors and apply best practices for success with roles.

> For best practices on designing record access in a large organization, see *Designing Record Access for Enterprise Scale*.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

- To simplify user management in organizations with large numbers of users, enable delegated administrators to manage users in specified roles and all subordinate roles.
- You can create up to 500 roles for your organization.
- Every user must be assigned to a role, or their data will not display in opportunity reports, forecast roll-ups, and other displays based on roles.
- All users that require visibility to the entire organization should belong to the highest level in the hierarchy.
- It is not necessary to create individual roles for each title at your company. Instead, define a hierarchy of roles to control access of information entered by users in lower level roles.
- When you change a user's role, the sharing rules for the new role are applied.
- If you are a Salesforce Knowledge user, you can modify category visibility settings on the role detail page.
- To avoid performance issues, no single user should own more than 10,000 records of an object. Users who need to own more than that number of objects should either not be assigned a role or placed in a separate role at the top of the hierarchy. It's also important to keep that user out of public groups that might be used as the source for sharing rules.

- When an account owner is not assigned a role, the sharing access for related contacts is Read/Write, provided the organization-wide default for contacts is not Controlled by Parent. Sharing access on related opportunities and cases is No Access.
- If your organization uses Territory Management, forecasts are based on the territory hierarchy rather than the role hierarchy.

Assign Users to Roles

Quickly assign users to a particular role.

1. From Setup, enter `Roles` in the `Quick Find` box, then select **Roles**.
2. Click **Assign** next to the name of the desired role.

   Note: You can also access this page by clicking **Assign Users to Role** from the Users in Role related list. Large organizations should consider assigning roles via the SOAP API for efficiency.

3. Make a selection from the drop-down list to show the available users.
4. Select a user on the left, and click **Add** to assign the user to this role.

Note: Removing a user from the Selected Users list deletes the role assignment for that user.

SEE ALSO:

User Role Hierarchy

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To assign users to roles:
- Manage Internal Users

Role Fields

The fields that comprise a role entry have specific purposes. Refer to this table for descriptions of each field and how it functions in a role.

The visibility of fields depends on your organization’s permissions and sharing settings.

Field	Description
`Case Access`	Specifies whether users can access other users’ cases that are associated with accounts the users own. This field is not visible if your organization’s sharing model for cases is Public Read/Write.
`Contact Access`	Specifies whether users can access other users’ contacts that are associated with accounts the users own. This field is not visible if your organization’s sharing model for contacts is Public Read/Write or Controlled by Parent.
`Label`	The name used to refer to the role or title of position in any user interface pages, for example, Western Sales VP.
`Modified By`	The name of the user who last modified this role's details, and the date and time that the role was modified.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create or edit roles:
- Manage Roles

Field	Description
`Opportunity Access`	Specifies whether users can access other users' opportunities that are associated with accounts the users own. This field is not visible if your organization's sharing model for opportunities is Public Read/Write.
`Partner Role`	Indicates whether this role is associated with a partner account. This field is available only when a Customer Portal or partner portal is enabled for the organization. If this checkbox is selected, you cannot edit the role. The default number of roles in portal accounts is three. You can reduce the number of roles or add roles to a maximum of three.
`Role Name`	The unique name used by the API and managed packages.
`Role Name as displayed on reports`	A role name that appears in reports. When editing a role, if the `Role Name` is long, you can enter an abbreviated name in this field.
`Sharing Groups`	These groups are automatically created and maintained. The Role group contains all users in this role plus all users in roles above this role. The Role and Subordinates group contains all users in this role plus all users in roles above and below this role in the hierarchy. The Role and Internal Subordinates group (available if Customer Portals or partner portals are enabled for your organization) contains all users in this role. It also contains all users in roles above and below this role, excluding Customer Portal and partner portal users.
`This role reports to`	The role above this role in the hierarchy.

SEE ALSO:

User Role Hierarchy

What Is a Group?

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

A group consists of a set of users. A group can contain individual users, other groups, or the users in a particular role or territory. It can also contain the users in a particular role or territory plus all the users below that role or territory in the hierarchy.

There are two types of groups.

Public groups

Administrators and delegated administrators can create public groups. Everyone in the organization can use public groups. For example, an administrator can create a group for an employee carpool program. All employees can then use this group to share records about the program.

Personal groups

Each user can create groups for their personal use. For example, users might need to ensure that certain records are always shared within a specified workgroup.

You can use groups in the following ways.

- To set up default sharing access via a sharing rule
- To share your records with other users
- To specify that you want to synchronize contacts owned by other users
- To add multiple users to a Salesforce CRM Content library
- To assign users to specific actions in Salesforce Knowledge

SEE ALSO:

Group Member Types

Create and Edit Groups

Viewing Group Lists

Sharing Records with Manager Groups

Public Group Considerations

Public Group Considerations

For organizations with a large number of users, consider these tips when creating public groups to optimize performance.

- Create a group when at least a few users need the same access.
- Create a group for members who don't need to frequently move in or out of the groups.
- Avoid creating groups within groups that result in more than five levels of nesting.
- Enable automatic access to records using role hierarchies for public groups by selecting **Grant Access Using Hierarchies** when creating the group. However, don't use this option if you're creating a public group with All Internal Users as members.

EDITIONS

Available in: Salesforce Classic

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

SEE ALSO:

What Is a Group?

Group Member Types

Many types of groups are available for various internal and external users.

When you create or edit a group, you can select the following types of members from the `Search` drop-down list. Depending on your organization settings, some types may not be available.

Member Type	Description
Customer Portal Users	All of your Customer Portal users. This is only available when a Customer Portal is enabled for your organization.
Partner Users	All of your partner users. This is only available when a partner portal is enabled for your organization.
Personal Groups	All of your own groups. This is only available when creating other personal groups.
Portal Roles	All roles defined for your organization's partner portal or Customer Portal. This includes all users in the specified portal role, except high-volume portal users. Note: A portal role name includes the name of the account that it's associated with, except for person accounts, which include the user `Alias`.
Portal Roles and Subordinates	All roles defined for your organization's partner portal or Customer Portal. This includes all of the users in the specified portal role plus all of the users below that role in the portal role hierarchy, except for high-volume portal users. Note: A portal role name includes the name of the account that it's associated with, except for person accounts, which include the user `Alias`.
Public Groups	All public groups defined by your administrator.
Roles	All roles defined for your organization. Adding a role to a group includes all of the users in that role, but does not include portal roles.
Roles and Internal Subordinates	Adding a role and its subordinate roles includes all of the users in that role plus all of the users in roles below that role. This doesn't include portal roles or users.
Roles and Subordinates	Adding a role and its subordinate roles includes all of the users in that role plus all of the users

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

The member types that are available vary depending on your Edition.

USER PERMISSIONS

To create or edit a public group:
- Manage Users

To create or edit another user's personal group:
- Manage Users

Member Type	Description
	in roles below that role. This is only available when no portals are enabled for your organization.
Roles, Internal and Portal Subordinates	Adding a role and its subordinate roles includes all of the users in that role plus all of the users in roles below that role. This is only available when a partner or Customer Portal is enabled for your organization. This includes portal users.
Users	All users in your organization. This doesn't include portal users.

SEE ALSO:

What Is a Group?

Sharing Records with Manager Groups

Create and Edit Groups

Only administrators and delegated administrators can create and edit public groups, but anyone can create and edit their own personal groups.

To create or edit a group:

1. Click the control that matches the type of group:
   - For personal groups, go to your personal settings and click **My Personal Information** or **Personal**—whichever one appears. Then click **My Groups**. The Personal Groups related list is also available on the user detail page.
   - For public groups, from Setup, enter *Public Groups* in the `Quick Find` box, then select **Public Groups**.
2. Click **New**, or click **Edit** next to the group you want to edit.
3. Enter the following:

Field	Description
`Label`	The name used to refer to the group in any user interface pages.
`Group Name` (public groups only)	The unique name used by the API and managed packages.
`Grant Access Using Hierarchies` (public groups only)	Select **Grant Access Using Hierarchies** to allow automatic access to records using your role hierarchies. When selected, any records shared with users in this group are also shared with users higher in the hierarchy. Deselect **Grant Access Using Hierarchies** if you're creating a public group with All Internal Users as members, which optimizes performance for sharing records with groups.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create or edit a public group:
- Manage Users

To create or edit another user's personal group:
- Manage Users

	Note: If **Grant Access Using Hierarchies** is deselected, users that are higher in the role hierarchy don't receive automatic access. However, some users—such as those with the "View All" and "Modify All" object permissions and the "View All Data" and "Modify All Data" system permissions—can still access records they don't own.
`Search`	From the `Search` drop-down list, select the type of member to add. If you don't see the member you want to add, enter keywords in the search box and click **Find**. Note: For account owners to see child records owned by high-volume portal users, they must be members of any portal share groups with access to the portal users' data.
`Selected Members`	Select members from the Available Members box, and click **Add** to add them to the group.
`Selected Delegated Groups`	In this list, specify any delegated administration groups whose members can add or remove members from this public group. Select groups from the Available Delegated Groups box, and then click **Add**. This list appears only in public groups.

4. Click **Save**.

Note: When you edit groups, roles, and territories, sharing rules are recalculated to add or remove access as needed.

SEE ALSO:

What Is a Group?

Viewing Group Lists

1. Click the control that matches the type of group.
   - For personal groups, in your personal settings, click **My Personal Information** or **Personal**—whichever one appears. Then click **My Groups**.
   - For public groups, from Setup, enter *`Public Groups`* in the `Quick Find` box, then select **Public Groups**.
2. Click the name of a group in the Groups related list to display the group's detail page.
   - To edit the group membership, click **Edit**.
   - To delete the group, click **Delete**.
   - To view active group members, see the Group Members related list.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To edit a public group:
- Manage Users

- To view all group members and users who have equivalent access because they are higher in the role or territory hierarchy, click **View All Users** to display the All Users in Group related list. Click **View Group Members** to return to the Group Members related list.

SEE ALSO:

What Is a Group?

Sharing Records with Manager Groups

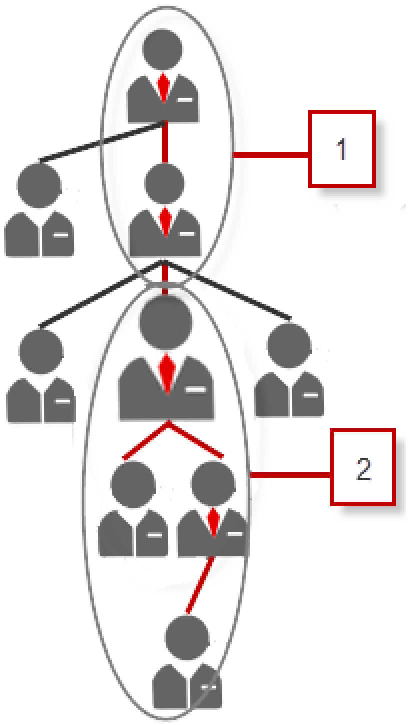
Share records up or down the management chain using sharing rules or manual sharing.

EDITIONS

Available in: Salesforce Classic

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

The role hierarchy controls the level of visibility that users have into your organization's data. With Spring '15, you can use manager groups to share records with your management chain, instead of all managers in the same role based on the role hierarchy. Manager groups can be used wherever other groups are used, such as in a manual share or sharing rule. But they cannot be added to other groups and don't include portal users. Manager groups can contain Standard and Chatter Only users only.



Every user has two manager groups—Managers Group (1) and Manager Subordinates Group (2)— where (1) includes a user's direct and indirect managers, and (2) includes a user and the user's direct and indirect reports. On a sharing rule setup page, these groups are available on the Share with drop-down list.

To find out who a user's manager is, from Setup, enter *Users* in the `Quick Find` box, then select **Users**. Click a user's name. The `Manager` field on the user detail page displays the user's manager.

To enable users to share records with the manager groups, follow these steps.

1. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
2. On the Sharing Settings page, click **Edit**.
3. In Other Settings, select `Manager Groups` and then click **Save**.

Note: You can't disable manager groups if your organization uses Work.com or have any sharing rules that uses manager groups.

With manager groups, you can share records to these groups via manual sharing, sharing rules, and Apex managed sharing. Apex sharing reasons is not supported. For Apex managed sharing, include the row cause ID, record ID, and the manager group ID. For more information, see the *Force.com Apex Code Developer's Guide*.

Inactive users remain in the groups of which they are members, but all relevant sharing rules and manual sharing are retained in the groups.

Note: If your organization has User Sharing enabled, you can't see the users whom you don't have access to. Additionally, a querying user who doesn't have access to another user can't query that user's groups.

Example: You might have a custom object for performance reviews whose organization-wide default is set to Private. After deselecting the `Grant Access Using Hierarchies` checkbox, only the employee who owns the review record can view and edit it. To share the reviews up the management chain, administrators can create a sharing rule that shares to a user's Managers Group. Alternatively, the employee can share the review record with the user's Managers Group by using manual sharing.

SEE ALSO:

Sharing Settings

Sharing Rules

Sharing Rule Categories

Sharing Rules

Make automatic exceptions to your organization-wide sharing settings for defined sets of users.

Note: Who Sees What: Record Access via Sharing Rules (English only)

Watch how you can grant access to records using sharing rules.

For example, use sharing rules to extend sharing access to users in public groups, roles, or territories. Sharing rules can never be stricter than your organization-wide default settings. They simply allow greater access for particular users.

You can create these types of sharing rules.

Type	Based on	Set Default Sharing Access for
Account sharing rules	Account owner or other criteria, including account record types or field values	Accounts and their associated contracts, opportunities, cases, and optionally, contacts and orders
Account territory sharing rules	Territory assignment	Accounts and their associated cases, contacts, contracts, and opportunities
Asset sharing rules	Asset owner or other criteria, including asset record types or field values	Individual assets
Campaign sharing rules	Campaign owner or other criteria, including campaign record types or field values	Individual campaigns
Case sharing rules	Case owner or other criteria, including case record types or field values	Individual cases and associated accounts
Contact sharing rules	Contact owner or other criteria, including contact record types or field values	Individual contacts and associated accounts
Custom object sharing rules	Custom object owner or other criteria, including custom object record types or field values	Individual custom object records
Lead sharing rules	Lead owner or other criteria, including lead record types or field values	Individual leads
Location sharing rules	Location owner only; criteria-based sharing rules aren’t available	Individual locations

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Account, asset, and contact sharing rules are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Account territory, case, lead, opportunity, order, and custom object sharing rules are available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Campaign sharing rules are available in **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions and in **Professional** Edition for an additional cost

Record types are available in **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Type	Based on	Set Default Sharing Access for
Opportunity sharing rules	Opportunity owner or other criteria, including opportunity record types or field values	Individual opportunities and their associated accounts
Order sharing rules	Order owner or other criteria, including order record types or field values	Individual orders
Product item sharing rules	Product item owner only; criteria-based sharing rules aren't available	Individual product items
Product request sharing rules	Product request owner only; criteria-based sharing rules aren't available	Individual product requests
Product transfer sharing rules	Product transfer owner only; criteria-based sharing rules aren't available	Individual product transfers
Service appointment sharing rules	Service appointment owner only; criteria-based sharing rules aren't available	Individual service appointments
Service contract sharing rules	Service contract owner only; criteria-based sharing rules aren't available	Individual service contracts
Service crew sharing rules	Service crew owner only; criteria-based sharing rules aren't available	Individual service crews
Service resource sharing rules	Service resource owner only; criteria-based sharing rules aren't available	Individual service resources
Service territory sharing rules	Service territory owner only; criteria-based sharing rules aren't available	Individual service territories
Shipment sharing rules	Shipment owner only; criteria-based sharing rules aren't available	Individual shipments
Time sheet sharing rules	Time sheet owner only; criteria-based sharing rules aren't available	Individual time sheets
User sharing rules	Group membership or other criteria, including username and whether the user is active	Individual users
User provisioning request sharing rules	User provisioning request owner, only; criteria-based sharing rules aren't available	Individual user provisioning requests
Work order sharing rules	Work order owner or other criteria, including work order record types or field values	Individual work orders
Work type sharing rules	Work type owner only; criteria-based sharing rules aren't available	Individual work types

Note:

- You can't include high-volume portal users in sharing rules because they don't have roles and can't be in public groups.

- Developers can use Apex to programmatically share custom objects (based on record owners, but not other criteria). This does not apply to User Sharing.

SEE ALSO:

Criteria-Based Sharing Rules

Sharing Rule Considerations

Criteria-Based Sharing Rules

Criteria-based sharing rules determine whom to share records with based on field values in records. For example, let's say you use a custom object for job applications, with a custom picklist field named "Department." A criteria-based sharing rule could share all job applications in which the Department field is set to "IT" with all IT managers in your organization.

Note:

- Although criteria-based sharing rules are based on values in the records and not the record owners, a role or territory hierarchy still allows users higher in the hierarchy to access the records.
- You can't use Apex to create criteria-based sharing rules. Also, criteria-based sharing cannot be tested using Apex.
- You can use the **SharingRules** type in the Metadata API to create criteria-based sharing rules starting in API version 24.0.
- You can't include high-volume portal users in sharing rules because they don't have roles and can't be in public groups.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Accounts, Opportunities, Cases, Contacts, and record types are not available in **Database.com**

You can create criteria-based sharing rules for accounts, assets, opportunities, cases, contacts, leads, campaigns, work orders, and custom objects. You can create up to 50 criteria-based sharing rules per object.

- Record types
- These field types:
  - Auto Number
  - Checkbox
  - Date
  - Date/Time
  - Email
  - Number
  - Percent
  - Phone
  - Picklist
  - Text
  - Text Area
  - URL
  - Lookup Relationship (to user ID or queue ID)

Note: Text and Text Area are case-sensitive. For example, a criteria-based sharing rule that specifies "Manager" in a text field doesn't share records that have "manager" in the field. To create a rule with several common cases of a word, enter each value separated by a comma.

SEE ALSO:

Sharing Rules

Sharing Rule Categories

When you define a sharing rule, you can choose from the following categories in the `owned by members of` and `Share with` drop-down lists. Depending on the type of sharing rule and the features enabled for your organization, some categories may not appear.

Note: You can't include high-volume portal users in sharing rules because they don't have roles and can't be in public groups.

Category	Description
Managers Groups	All direct and indirect managers of a user.
Manager Subordinates Groups	A manager and all direct and indirect reports who he or she manages.
Queues	All records owned by the queue, excluding records owned by individual members of the queue. Available only in the `owned by members of` list.
Public Groups	All public groups defined by your administrator. If a partner portal or Customer Portal is enabled for your organization, the All Partner Users or All Customer Portal Users group displays. These groups includes all users allowed to access your partner portal or Customer Portal, except for high-volume portal users.
Roles	All roles defined for your organization. This includes all of the users in the specified role.
Portal Roles	All roles defined for your organization's partner portal or Customer Portal. This includes all users in the specified portal role, except high-volume portal users. A portal role name includes the name of the account that it's associated with, except for person accounts, which include the user `Alias`.
Roles and Subordinates	All roles defined for your organization. This includes all of the users in the specified role plus all of the users in roles below that role, including partner portal and Customer Portal roles that contain users with a portal license type. Portal roles are only included in this category if a partner portal or Customer Portal is enabled for your organization.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Account and contact sharing rules available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Account territory, case, lead, and opportunity sharing rules available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Campaign sharing rules available in **Professional** Edition for an additional cost, and **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Custom object sharing rules available in: **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions.

Partner Portals and Customer Portals available in Salesforce Classic

Category	Description
	The Roles, Internal and Portal Subordinates data set category is only available in your organization after you create at least one role in the role hierarchy.
Portal Roles and Subordinates	All roles defined for your organization's partner portal or Customer Portal. This includes all of the users in the specified portal role plus all of the users below that role in the portal role hierarchy, except for high-volume portal users. A portal role name includes the name of the account that it's associated with, except for person accounts, which include the user `Alias`.
Roles and Internal Subordinates	All roles defined for your organization. This includes all of the users in the specified role plus all of the users in roles below that role, excluding partner portal and Customer Portal roles. This category only displays if a partner portal or Salesforce Customer Portal is enabled for your organization. The Roles and Internal Subordinates data set category is only available in your organization after you create at least one role in the role hierarchy *and* enable a portal.
Roles, Internal and Portal Subordinates	All roles defined for your organization. This includes all of the users in the specified role plus all of the users in roles below that role, including partner portal and Customer Portal roles. This category only displays if a partner portal or Salesforce Customer Portal is enabled for your organization. The Roles and Internal Subordinates data set category is only available in your organization after you create at least one role in the role hierarchy *and* enable a portal.
Territories	All territories defined for your organization.
Territories and Subordinates	All territories defined for your organization. This includes the specified territory plus all territories below it.

SEE ALSO:

Sharing Rules

Sharing Records with Manager Groups

Creating Lead Sharing Rules

Lead sharing rules are based on the record owner or on other criteria, including record type and certain field values. You can define up to 300 lead sharing rules, including up to 50 criteria-based sharing rules.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create sharing rules:

- Manage Sharing

1. If you plan to include public groups in your sharing rule, confirm that the appropriate groups have been created.
2. From Setup, enter *`Sharing Settings`* in the `Quick Find` box, then select **Sharing Settings**.
3. In the Lead Sharing Rules related list, click **New**.
4. Enter the **Label Name** and **Rule Name**. The Label is the sharing rule label as it appears on the user interface. The Rule Name is a unique name used by the API and managed packages.
5. Enter the **Description**. This field describes the sharing rule. It is optional and can contain up to 1000 characters.
6. Select a rule type.
7. Depending on the rule type you selected, do the following:
   - `Based on record owner`—In the `owned by members of` line, specify the users whose records will be shared: select a category from the first drop-down list and a set of users from the second drop-down list (or lookup field, if your organization has over 200 queues, groups, roles, or territories).
   - `Based on criteria`—Specify the Field, Operator, and Value criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value is always a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.

     Note: To use a field that's not supported by criteria-based sharing rules, you can create a workflow rule or Apex trigger to copy the value of the field into a text or numeric field, and use that field as the criterion.
8. In the `Share with` line, specify the users who get access to the data: select a category from the first drop-down list and a set of users from the second drop-down list or lookup field.
9. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

10. Click **Save**.

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Editing Lead Sharing Rules

For sharing rules that are based on owner, you can edit only the sharing access settings. For sharing rules that are based on other criteria, you can edit the criteria and sharing access settings.

1. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
2. In the Lead Sharing Rules related list, click **Edit** next to the rule you want to change.
3. Change the Label and Rule Name if desired.
4. If you selected a rule that's based on owner, skip to the next step.

   If you selected a rule that's based on criteria, specify the criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value must be a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.
5. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

6. Click **Save**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit sharing rules:
- Manage Sharing

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Creating Account Sharing Rules

Account sharing rules can be based on the record owner or on other criteria, including record type and certain field values. You can define up to 300 account sharing rules, including up to 50 criteria-based sharing rules.

1. If you plan to include public groups in your sharing rule, confirm that the appropriate groups have been created.
2. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
3. In the Account Sharing Rules related list, click **New**.
4. Enter the **Label Name** and **Rule Name**. The Label is the sharing rule label as it appears on the user interface. The Rule Name is a unique name used by the API and managed packages.
5. Enter the **Description**. This field describes the sharing rule. It is optional and can contain up to 1000 characters.
6. Select a rule type.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create sharing rules:
- Manage Sharing

7. Depending on the rule type you selected, do the following:
   - `Based on record owner`—In the `owned by members of` line, specify the users whose records will be shared: select a category from the first drop-down list and a set of users from the second drop-down list (or lookup field, if your organization has over 200 queues, groups, roles, or territories).
   - `Based on criteria`—Specify the Field, Operator, and Value criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value is always a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.

     Note: To use a field that's not supported by criteria-based sharing rules, you can create a workflow rule or Apex trigger to copy the value of the field into a text or numeric field, and use that field as the criterion.

8. In the `Share with` line, specify the users who get access to the data: select a category from the first drop-down list and a set of users from the second drop-down list or lookup field.
9. Select a setting for `Default Account, Contract and Asset Access`.
10. In the remaining fields, select the access settings for the records associated with the shared accounts.

Access Setting	Description
Private (available for associated contacts, opportunities, and cases only)	Users can't view or update records, unless access is granted outside of this sharing rule.
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

Note: `Contact Access` is not available when the organization-wide default for contacts is set to Controlled by Parent.

11. Click **Save**.

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Editing Account Sharing Rules

For sharing rules that are based on owner, you can edit only the sharing access settings. For sharing rules that are based on other criteria, you can edit the criteria and sharing access settings.

1. From Setup, enter *`Sharing Settings`* in the `Quick Find` box, then select **Sharing Settings**.
2. In the Account Sharing Rules related list, click **Edit** next to the rule you want to change.
3. Change the Label and Rule Name if desired.
4. If you selected a rule that's based on owner, skip to the next step.

   If you selected a rule that's based on criteria, specify the criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value must be a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.
5. Select a setting for `Default Account, Contract and Asset Access`.
6. In the remaining fields, select the access settings for the records associated with the shared accounts.

Access Setting	Description
Private (available for associated contacts, opportunities, and cases only)	Users can't view or update records, unless access is granted outside of this sharing rule.
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

Note: `Contact Access` is not available when the organization-wide default for contacts is set to Controlled by Parent.

7. Click **Save**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit sharing rules:
- Manage Sharing

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Creating Account Territory Sharing Rules

Account territory sharing rules are based on territory assignment. You can define up to 300 account territory sharing rules.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create sharing rules:

- Manage Sharing

1. If you plan to include public groups in your sharing rule, confirm that the appropriate groups have been created.
2. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
3. In the Account Territory Sharing Rules related list, click **New**.
4. Enter the **Label Name** and **Rule Name**. The Label is the sharing rule label as it appears on the user interface. The Rule Name is a unique name used by the API and managed packages.
5. Enter the **Description**. This field describes the sharing rule. It is optional and can contain up to 1000 characters.
6. In the Accounts in Territory line, select Territories or Territories and Subordinates from the first drop-down list and a territory from the second drop-down list.
7. In the `Share with` line, specify the users who get access to the data: select a category from the first drop-down list and a set of users from the second drop-down list or lookup field.
8. Select a setting for `Default Account, Contract and Asset Access`.
9. In the remaining fields, select the access setting for the records associated with the shared account territories.

Access Setting	Description
Private (available for associated contacts, opportunities, and cases only)	Users can't view or update records, unless access is granted outside of this sharing rule.
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

Note: `Contact Access` is not available when the organization-wide default for contacts is set to Controlled by Parent.

10. Click **Save**.

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Editing Account Territory Sharing Rules

For account territory sharing rules, you can edit the sharing access settings, but no other settings.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit sharing rules:
- Manage Sharing

1. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
2. In the Account Territory Sharing Rules related list, click **Edit** next to the rule you want to change.
3. Change the Label and Rule Name if desired.
4. Select the sharing access setting for users.

Access Setting	Description
Private (available for associated contacts, opportunities, and cases only)	Users can't view or update records, unless access is granted outside of this sharing rule.
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

Note: `Contact Access` is not available when the organization-wide default for contacts is set to Controlled by Parent.

5. Click **Save**.

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Create Contact Sharing Rules

Make automatic exceptions to your contact organization-wide sharing settings for defined sets of users.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create sharing rules:
- Manage Sharing

Contact sharing rules can be based on the record owner or on other criteria, including record type and certain field values. You can define up to 300 contact sharing rules, including up to 50 criteria-based sharing rules.

1. If you plan to include public groups in your sharing rule, confirm that the appropriate groups have been created.
2. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
3. In the Contact Sharing Rules related list, click **New**.
4. Enter the **Label Name** and **Rule Name**. The Label is the sharing rule label as it appears on the user interface. The Rule Name is a unique name used by the API and managed packages.
5. Enter the **Description**. This field describes the sharing rule. It is optional and can contain up to 1000 characters.

6. Select a rule type.
7. Depending on the rule type you selected, do the following:
   - `Based on record owner`—In the `owned by members of` line, specify the users whose records will be shared: select a category from the first drop-down list and a set of users from the second drop-down list (or lookup field, if your organization has over 200 queues, groups, roles, or territories).
   - `Based on criteria`—Specify the Field, Operator, and Value criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value is always a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.

     Note: To use a field that's not supported by criteria-based sharing rules, you can create a workflow rule or Apex trigger to copy the value of the field into a text or numeric field, and use that field as the criterion.
8. In the `Share with` line, specify the users who get access to the data: select a category from the first drop-down list and a set of users from the second drop-down list or lookup field.
9. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

10. Click **Save**.

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Editing Contact Sharing Rules

For sharing rules that are based on owner, you can edit only the sharing access settings. For sharing rules that are based on other criteria, you can edit the criteria and sharing access settings.

1. From Setup, enter *`Sharing Settings`* in the `Quick Find` box, then select **Sharing Settings**.
2. In the Contact Sharing Rules related list, click **Edit** next to the rule you want to change.
3. Change the Label and Rule Name if desired.
4. If you selected a rule that's based on owner, skip to the next step.

   If you selected a rule that's based on criteria, specify the criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value must be a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.
5. Select the sharing access setting for users.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit sharing rules:

- Manage Sharing

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

6. Click **Save**.

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Creating Opportunity Sharing Rules

Opportunity sharing rules can be based on the record owner or on other criteria, including record type and certain field values. You can define up to 300 opportunity sharing rules, including up to 50 criteria-based sharing rules.

1. If you plan to include public groups in your sharing rule, confirm that the appropriate groups have been created.
2. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
3. In the Opportunity Sharing Rules related list, click **New**.
4. Enter the **Label Name** and **Rule Name**. The Label is the sharing rule label as it appears on the user interface. The Rule Name is a unique name used by the API and managed packages.
5. Enter the **Description**. This field describes the sharing rule. It is optional and can contain up to 1000 characters.
6. Select a rule type.
7. Depending on the rule type you selected, do the following:
   - `Based on record owner`—In the `owned by members of` line, specify the users whose records will be shared: select a category from the first drop-down list and a set of users from the second drop-down list (or lookup field, if your organization has over 200 queues, groups, roles, or territories).
   - `Based on criteria`—Specify the Field, Operator, and Value criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value is always a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.

     Note: To use a field that's not supported by criteria-based sharing rules, you can create a workflow rule or Apex trigger to copy the value of the field into a text or numeric field, and use that field as the criterion.
8. In the `Share with` line, specify the users who get access to the data: select a category from the first drop-down list and a set of users from the second drop-down list or lookup field.
9. Select the sharing access setting for users. For owner-based rules or criteria-based rules with ownership as criteria, the `Opportunity Access` level applies to opportunities owned by the group, role, or territory members, regardless of the associated account.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create sharing rules:

- Manage Sharing

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

10. Click **Save**.

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Editing Opportunity Sharing Rules

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit sharing rules:

- Manage Sharing

For sharing rules that are based on owner, you can edit only the sharing access settings. For sharing rules that are based on other criteria, you can edit the criteria and sharing access settings.

1. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
2. In the Opportunity Sharing Rules related list, click **Edit** next to the rule you want to change.
3. Change the Label and Rule Name if desired.
4. If you selected a rule that's based on owner, skip to the next step.

   If you selected a rule that's based on criteria, specify the criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value must be a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.

5. Select the sharing access setting for users. For owner-based rules or criteria-based rules with ownership as criteria, the `Opportunity Access` level applies to opportunities owned by the group, role, or territory members, regardless of the associated account.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

6. Click **Save**.

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Creating Case Sharing Rules

Case sharing rules can be based on the record owner or on other criteria, including record type and certain field values. You can define up to 300 case sharing rules, including up to 50 criteria-based sharing rules.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create sharing rules:

- Manage Sharing

1. If you plan to include public groups in your sharing rule, confirm that the appropriate groups have been created.
2. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
3. In the Case Sharing Rules related list, click **New**.
4. Enter the **Label Name** and **Rule Name**. The Label is the sharing rule label as it appears on the user interface. The Rule Name is a unique name used by the API and managed packages.
5. Enter the **Description**. This field describes the sharing rule. It is optional and can contain up to 1000 characters.
6. Select a rule type.
7. Depending on the rule type you selected, do the following:
   - `Based on record owner`—In the `owned by members of` line, specify the users whose records will be shared: select a category from the first drop-down list and a set of users from the second drop-down list (or lookup field, if your organization has over 200 queues, groups, roles, or territories).
   - `Based on criteria`—Specify the Field, Operator, and Value criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value is always a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.

     Note: To use a field that's not supported by criteria-based sharing rules, you can create a workflow rule or Apex trigger to copy the value of the field into a text or numeric field, and use that field as the criterion.
8. In the `Share with` line, specify the users who get access to the data: select a category from the first drop-down list and a set of users from the second drop-down list or lookup field.
9. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

10. Click **Save**.

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Editing Case Sharing Rules

For sharing rules that are based on owner, you can edit only the sharing access settings. For sharing rules that are based on other criteria, you can edit the criteria and sharing access settings.

1. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
2. In the Case Sharing Rules related list, click **Edit** next to the rule you want to change.
3. Change the Label and Rule Name if desired.
4. If you selected a rule that's based on owner, skip to the next step.

   If you selected a rule that's based on criteria, specify the criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value must be a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.

5. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

6. Click **Save**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit sharing rules:
- Manage Sharing

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Creating Campaign Sharing Rules

Campaign sharing rules can be based on the record owner or on other criteria, including record type and certain field values. You can define up to 300 campaign sharing rules, including up to 50 criteria-based sharing rules.

1. If you plan to include public groups in your sharing rule, confirm that the appropriate groups have been created.
2. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
3. In the Campaign Sharing Rules related list, click **New**.
4. Enter the **Label Name** and **Rule Name**. The Label is the sharing rule label as it appears on the user interface. The Rule Name is a unique name used by the API and managed packages.
5. Enter the **Description**. This field describes the sharing rule. It is optional and can contain up to 1000 characters.
6. Select a rule type.

EDITIONS

Available in: Salesforce Classic

Available in: **Professional** Edition for an additional cost, and **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To create sharing rules:
- Manage Sharing

7. Depending on the rule type you selected, do the following:
    - `Based on record owner`—In the `owned by members of` line, specify the users whose records will be shared: select a category from the first drop-down list and a set of users from the second drop-down list (or lookup field, if your organization has over 200 queues, groups, roles, or territories).
    - `Based on criteria`—Specify the Field, Operator, and Value criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value is always a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.

      Note: To use a field that's not supported by criteria-based sharing rules, you can create a workflow rule or Apex trigger to copy the value of the field into a text or numeric field, and use that field as the criterion.

8. In the `Share with` line, specify the users who get access to the data: select a category from the first drop-down list and a set of users from the second drop-down list or lookup field.
9. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.
Full Access	Any user in the selected group, role, or territory can view, edit, transfer, delete, and share the record, just like the record's owner. With a Full Access sharing rule, users can also view, edit, delete, and close activities associated with the record if the organization-wide sharing setting for activities is Controlled by Parent.

10. Click **Save**.

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Editing Campaign Sharing Rules

For sharing rules that are based on owner, you can edit only the sharing access settings. For sharing rules that are based on other criteria, you can edit the criteria and sharing access settings.

1. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
2. In the Campaign Sharing Rules related list, click **Edit** next to the rule you want to change.
3. Change the Label and Rule Name if desired.
4. If you selected a rule that's based on owner, skip to the next step.

   If you selected a rule that's based on criteria, specify the criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value must be a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.

5. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.
Full Access	Any user in the selected group, role, or territory can view, edit, transfer, delete, and share the record, just like the record’s owner. With a Full Access sharing rule, users can also view, edit, delete, and close activities associated with the record if the organization-wide sharing setting for activities is Controlled by Parent.

6. Click **Save**.

EDITIONS

Available in: Salesforce Classic

Available in: **Professional** Edition for an additional cost, and **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To edit sharing rules:

- Manage Sharing

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Creating Quick Text Sharing Rules

To create Quick Text sharing rules:

1. If you plan to include public groups in your sharing rule, confirm that the appropriate groups have been created.
2. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
3. In the Quick Text Sharing Rules related list, click **New**.
4. Enter the **Label Name** and **Rule Name**. The Label is the sharing rule label as it appears on the user interface. The Rule Name is a unique name used by the API and managed packages.
5. Enter the **Description**. This field describes the sharing rule. It is optional and can contain up to 1000 characters.
6. In the `Quick Text: owned by members of` line, specify the users who own the data by selecting a category from the first drop-down list and a set of users from the second drop-down list.
7. In the `Share with` line, specify the users who get access to the data: select a category from the first drop-down list and a set of users from the second drop-down list or lookup field.
8. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

9. Click **Save**.

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To create sharing rules:
- Manage Sharing

Creating Custom Object Sharing Rules

Custom object sharing rules can be based on the record owner or on other criteria, including record type and certain field values. You can define up to 300 custom object sharing rules, including up to 50 criteria-based sharing rules.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create sharing rules:

- Manage Sharing

1. If you plan to include public groups in your sharing rule, confirm that the appropriate groups have been created.
2. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
3. In the Sharing Rules related list for the custom object, click **New**.
4. Enter the Label and Rule Name. The Label is the sharing rule label as it appears on the user interface. The Rule Name is a unique name used by the API and managed packages.
5. Enter the **Description**. This field describes the sharing rule. It is optional and can contain up to 1000 characters.
6. Select a rule type.
7. Depending on the rule type you selected, do the following:
   - `Based on record owner`—In the `owned by members of` line, specify the users whose records will be shared: select a category from the first drop-down list and a set of users from the second drop-down list (or lookup field, if your organization has over 200 queues, groups, roles, or territories).
   - `Based on criteria`—Specify the Field, Operator, and Value criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value is always a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.

     Note: To use a field that's not supported by criteria-based sharing rules, you can create a workflow rule or Apex trigger to copy the value of the field into a text or numeric field, and use that field as the criterion.
8. In the `Share with` line, specify the users who get access to the data: select a category from the first drop-down list and a set of users from the second drop-down list or lookup field.
9. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

10. Click **Save**.

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Editing Custom Object Sharing Rules

For sharing rules that are based on owner, you can edit only the sharing access settings. For sharing rules that are based on other criteria, you can edit the criteria and sharing access settings.

1. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
2. In the Sharing Rules related list for the custom object, click **Edit** next to the rule you want to change.
3. Change the Label and Rule Name if desired.
4. If you selected a rule that's based on owner, skip to the next step.

   If you selected a rule that's based on criteria, specify the criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value must be a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.

5. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

6. Click **Save**.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To edit sharing rules:
- Manage Sharing

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Create Order Sharing Rules

Order sharing rules can be based on the record owner or on other criteria, including record type and certain field values. You can define up to 300 order sharing rules, including up to 50 criteria-based sharing rules.

1. If you plan to include public groups in your sharing rule, confirm that the appropriate groups have been created.
2. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
3. In the Order Sharing Rules related list, click **New**.
4. Enter the **Label Name** and **Rule Name**. The Label is the sharing rule label as it appears on the user interface. The Rule Name is a unique name used by the API and managed packages.
5. Enter the **Description**. This field describes the sharing rule. It is optional and can contain up to 1000 characters.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To create sharing rules:
- Manage Sharing

6. Select a rule type.
7. Depending on the rule type you selected, do the following:
   - `Based on record owner`—In the `owned by members of` line, specify the users whose records will be shared: select a category from the first drop-down list and a set of users from the second drop-down list (or lookup field, if your organization has over 200 queues, groups, roles, or territories).
   - `Based on criteria`—Specify the Field, Operator, and Value criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value is always a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.

     Note: To use a field that's not supported by criteria-based sharing rules, you can create a workflow rule or Apex trigger to copy the value of the field into a text or numeric field, and use that field as the criterion.
8. In the `Share with` line, specify the users who get access to the data: select a category from the first drop-down list and a set of users from the second drop-down list or lookup field.
9. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

10. Click **Save**.

Edit Order Sharing Rules

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To edit sharing rules:
- Manage Sharing

For sharing rules that are based on owner, you can edit only the sharing access settings. For sharing rules that are based on other criteria, you can edit the criteria and sharing access settings.

1. From Setup, enter *`Sharing Settings`* in the `Quick Find` box, then select **Sharing Settings**.
2. In the Order Sharing Rules related list, click **Edit** next to the rule you want to change.
3. Change the Label and Rule Name if desired.
4. If you selected a rule that's based on owner, skip to the next step.

   If you selected a rule that's based on criteria, specify the criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value must be a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.
5. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

6. Click **Save**.

Creating User Provisioning Request Sharing Rules

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To create user provisioning request sharing rules:

- Manage Sharing and Use Identity Features

User provisioning request sharing rules can be based on the record owner, only. You can't create criteria-based user provisioning request sharing rules. You can define up to 300 user provisioning request sharing rules.

1. If you plan to include public groups in your sharing rule, confirm that the appropriate groups have been created.
2. From Setup, enter *Sharing Settings* in the `Quick Find` box, then select **Sharing Settings**.
3. In the User Provisioning Request Sharing Rules related list, click **New**.
4. Enter the **Label Name** and **Rule Name**. The Label is the sharing rule label as it appears on the user interface. The Rule Name is a unique name used by the API and managed packages.
5. Enter the **Description**. This field describes the sharing rule. It is optional and can contain up to 1000 characters.
6. In the `owned by members of` line, specify the users whose records are shared. Select a category from the first drop-down list and a set of users from the second drop-down list (or lookup field, if your organization has over 200 queues, groups, roles, or territories).
7. In the `Share with` line, specify the users who get access to the data: select a category from the first drop-down list and a set of users from the second drop-down list or lookup field.
8. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

9. Click **Save**.

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

Editing User Provisioning Request Sharing Rules

User Provisioning for Connected Apps

Editing User Provisioning Request Sharing Rules

For sharing rules that are based on an owner, you can edit only the sharing access settings. You can't create criteria-based user provisioning request sharing rules.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To edit sharing rules:

- Manage Sharing

1. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
2. In the User Provisioning Request Sharing Rules related list, click **Edit** next to the rule you want to change.
3. Change the Label and Rule Name if desired.
4. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

5. Click **Save**.

SEE ALSO:

Sharing Rules

Sharing Rule Considerations

Sharing Rule Categories

User Provisioning for Connected Apps

Create Work Order Sharing Rules

Work order sharing rules are based on the record owner or on other criteria, including record type and certain field values. You can define up to 300 work order sharing rules, including up to 50 criteria-based sharing rules.

EDITIONS

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

USER PERMISSIONS

To create sharing rules:

- Manage Sharing

To enable work orders:

- Customize Application

1. If you plan to include public groups in your sharing rule, confirm that the appropriate groups have been created.
2. From Setup, enter `Sharing Settings` in the Quick Find box, then select **Sharing Settings**.
3. In the Work Order Sharing Rules related list, click **New**.
4. Enter the **Label Name** and click the **Rule Name** field to auto-populate it.
5. Enter the **Description**. This field describes the sharing rule. It is optional and can contain up to 1000 characters.
6. Select a rule type.
7. Depending on the rule type you selected, do the following:
   - `Based on record owner`—In the owned by members of line, specify the users whose records are shared: select a category from the first drop-down list and a set of users from the second drop-down list (or lookup field, if your organization has over 200 queues, groups, roles, or territories).

- `Based on criteria`—Specify the Field, Operator, and Value criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value is always a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.

  Note: To use a field that's not supported by criteria-based sharing rules, you can create a workflow rule or Apex trigger to copy the value of the field into a text or numeric field, and use that field as the criterion.

8. In the **Share with** line, specify the users who get access to the data: select a category from the first drop-down list and a set of users from the second drop-down list or lookup field.
9. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

10. Click **Save**.

Sharing Rule Considerations

Sharing rules allow you to selectively grant data access to defined sets of users. Review the following notes before using sharing rules:

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Account and contact sharing rules are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Account territory, case, lead, opportunity, order, and custom object sharing rules are available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Campaign sharing rules are available in **Professional** Edition for an additional cost, and **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Only custom object sharing rules are available in **Database.com**

Granting Access

- You can use sharing rules to grant wider access to data. You cannot restrict access below your organization-wide default levels.
- If multiple sharing rules give a user different levels of access to a record, the user gets the most permissive access level.
- Sharing rules automatically grant additional access to related records. For example, opportunity sharing rules give role or group members access to the account associated with the shared opportunity if they do not already have it. Likewise, contact and case sharing rules provide the role or group members with access to the associated account as well.
- Users in the role hierarchy are automatically granted the same access that users below them in the hierarchy have from a sharing rule, provided that the object is a standard object or the **Grant Access Using Hierarchies** option is selected.
- Regardless of sharing rules, users can, at a minimum, view the accounts in their territories. Also, users can be granted access to view and edit the contacts, opportunities, and cases associated with their territories' accounts.

Updating

- Creating an owner-based sharing rule with the same source and target groups as an existing rule overwrites the existing rule.
- Once a sharing rule has been saved, you can't change the `Share with` field settings when you edit the sharing rule.
- Sharing rules apply to all new and existing records that meet the definition of the source data set.
- Sharing rules apply to both active and inactive users.

- When you change the access levels for a sharing rule, all existing records are automatically updated to reflect the new access levels.
- When you delete a sharing rule, the sharing access created by that rule is automatically removed.
- When you modify which users are in a group, role, or territory, the sharing rules are reevaluated to add or remove access as necessary.
- When you transfer records from one user to another, the sharing rules are reevaluated to add or remove access to the transferred records as necessary.
- Making changes to sharing rules may require changing a large number of records at once. To process these changes efficiently, your request may be queued and you may receive an email notification when the process has completed.
- Lead sharing rules do not automatically grant access to lead information after leads are converted into account, contact, and opportunity records.

Portal Users

- You can create rules to share records between most types of Customer Portal users and Salesforce users. Similarly, you can create sharing rules between Customer Portal users from different accounts as long as they have the Customer Portal Manager user license. However, you can't include high-volume portal users in sharing rules because they don't have roles and can't be in public groups.
- You can easily convert sharing rules that include Roles, Internal and Portal Subordinates to include Roles and Internal Subordinates instead by using the Convert Portal User Access wizard. Furthermore, you can use this wizard to convert any publicly accessible report, dashboard, and document folders to folders that are accessible by all users except for portal users.

Managed Package Fields

If a criteria-based sharing rule references a field from a licensed managed package whose license has expired, `(expired)` is appended to the label of the field. The field label is displayed in the field drop-down list on the rule's definition page in Setup. Criteria-based sharing rules that reference expired fields aren't recalculated, and new records aren't shared based on those rules. However, the sharing of existing records prior to the package's expiration is preserved.

SEE ALSO:

Sharing Rules

Sharing Rules for Communities

User Sharing

User Sharing enables you to show or hide an internal or external user from another user in your organization.

Watch a demo: Who Sees Whom: User Sharing (English only)

For example, you might be a manufacturer who wants to include all dealers in your organization but keep them from seeing or interacting with each other. If so, set the organization-wide defaults for the user object to Private. Then, open up access to specified dealers with sharing rules or manual sharing.

With User Sharing, you can:

- Assign the "View All Users" permission to users who need to see or interact with all users. This permission is automatically enabled for users who have the "Manage Users" permission.
- Set the organization-wide default for user records to Private or Public Read Only.
- Create user sharing rules based on group membership or other criteria.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Manual sharing, portals, and communities available in: Salesforce Classic

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

- Create manual shares for user records to open up access to individual users or groups.
- Control the visibility of external users in customer or partner portals and communities.

SEE ALSO:

Understanding User Sharing

Restoring User Visibility Defaults

Controlling Who Community or Portal Users Can See

Understanding User Sharing

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Manual sharing available in: Salesforce Classic

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

Set organization-wide defaults for internal and external user records. Then, extend access using sharing rules based on membership to public groups, roles, or territories, or use manual sharing to share individual user records with other users or groups.

When you enable user sharing, users can see other users in search, list views, and so on only if they have Read access on those users.

Review these considerations before you implement user sharing.

“View All Users” permission

This permission can be assigned to users who need Read access to all users, regardless of the sharing settings. If you already have the “Manage Users” permission, you are automatically granted the “View All Users” permission.

Organization-wide defaults for user records

This setting defaults to Private for external users and Public Read Only for internal users. When the default access is set to Private, users can only read and edit their own user record. Users with subordinates in the role hierarchy maintain read access to the user records of those subordinates.

User sharing rules

General sharing rule considerations apply to user sharing rules. User sharing rules are based on membership to a public group, role, or territory. Each sharing rule shares members of a source group with those of the target group. You must create the appropriate public groups, roles, or territories before creating your sharing rules. Users inherit the same access as users below them in the role hierarchy.

Manual sharing for user records

Manual sharing can grant read or edit access on an individual user, but only if the access is greater than the default access for the target user. Users inherit the same access as users below them in the role hierarchy. Apex managed sharing is not supported.

User sharing for external users

Users with the “Manage External Users” permission have access to external user records for Partner Relationship Management, Customer Service, and Customer Self-Service portal users, regardless of sharing rules or organization-wide default settings for User records. The “Manage External Users” permission does not grant access to guest or Chatter External users

User Sharing Compatibility

When the organization-wide default for the user object is set to Private, User Sharing does not fully support these features.

- Chatter Messenger is not available for external users. It is available for internal users only when the organization-wide default for the user object is set to Public Read Only.
- Customizable Forecasts—Users with the "View All Forecast" permission can see users to whom they don't have access.
- Salesforce CRM Content—A user who can create libraries can see users they don't have access to when adding library members.

- Standard Report Types—Some reports based on standard report types expose data of users to whom a user doesn't have access. For more information, see Control Standard Report Visibility.

SEE ALSO:

User Sharing

Set the Org-Wide Sharing Defaults for User Records

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To set default sharing access:

- Manage Sharing

Set the org-wide sharing defaults for the user object before opening up access.

For user records, you can set the organization-wide sharing default to Private or Public Read Only. The default must be set to Private if there is at least one user who shouldn't see a record.

Let's say that your organization has internal users (employees and sales agents) and external users (customers/portal users) under different sales agents or portal accounts, with these requirements:

- Employees can see everyone.
- Sales agents can see employees, other agents, and their own customer user records only.
- Customers can see other customers only if they are under the same agent or portal account.

To meet these requirements, set the default external access to Private, and extend access using sharing rules, manual sharing, or user permissions.

When the feature is first turned on, the default access setting is Private for external users. The default for internal users is Public Read Only. To change the organization-wide defaults for external access to the user object:

1. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
2. Click **Edit** in the Organization-Wide Defaults area.
3. Select the default internal and external access you want to use for user records.

   The default external access must be more restrictive or equal to the default internal access.
4. Click **Save**.

   Users have Read access to those below them in the role hierarchy and full access on their own user record.

SEE ALSO:

External Organization-Wide Defaults Overview

Controlling Who Community or Portal Users Can See

User Sharing

Creating User Sharing Rules

Share members of a group to members of another group, or share users based on criteria.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create sharing rules:

- Manage Sharing

User sharing rules can be based on membership to public groups, roles, or territories, or on other criteria such as Department and Title. By default, you can define up to 300 user sharing rules, including up to 50 criteria-based sharing rules. Contact Salesforce for information about increasing these limits.

User sharing rules based on membership enable user records belonging to members of one group to be shared with members of another group. Before you can create a membership-based user sharing rule, confirm that the appropriate groups have been created.

Users inherit the same access as users below them in the role hierarchy.

1. From Setup, enter *`Sharing Settings`* in the `Quick Find` box, then select **Sharing Settings**.
2. In the User Sharing Rules related list, click **New**.
3. Enter the **Label Name** and click the **Rule Name** field to auto-populate it.
4. Enter the **Description**. This field describes the sharing rule. It is optional and can contain up to 1000 characters.
5. Select a rule type.
6. Depending on the rule type you selected, do the following:
    a. `Based on group membership`—Users who are members of a group can be shared with members of another group. In the `Users who are members of` line, select a category from the first drop-down list and a set of users from the second drop-down list (or lookup field, if your organization has over 200 groups, roles, or territories).
    b. `Based on criteria`—Specify the Field, Operator, and Value criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value is always a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.
7. In the `Share with` line, specify the group that should have access to the user records. Select a category from the first drop-down list and a set of users from the second drop-down list or lookup field.
8. Select the sharing access setting for users.

Access Setting	Description
Read Only	Users can view, but not update, records. They can see target users in list views, lookups, search, and interact with them on Chatter.
Read/Write	Users can view and update records.

9. Click **Save**.

SEE ALSO:

Editing User Sharing Rules

Sharing Rule Categories

User Sharing

Editing User Sharing Rules

For user sharing rules based on membership to groups, roles, or territories, you can edit only the access settings. For user sharing rules based on other criteria, you can edit the criteria and access settings.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit sharing rules:

- Manage Sharing

1. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
2. In the User Sharing Rules related list, click **Edit** next to the rule you want to change.
3. Change the Label and Rule Name if desired.
4. If you selected a rule that's based on group membership, skip to the next step. If you selected a rule that's based on criteria, specify the criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value must be a literal number or string. Click **Add Filter Logic...** to change the default AND relationship between each filter.
5. Select the sharing access setting for users. The **User Access** level applies to users who are members of the groups being shared to.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

6. Click **Save**.

SEE ALSO:

User Sharing

Share User Records

Your administrator defines your organization's sharing model and default access levels for user records. If the organization-wide default access is set to Private or Public Read Only, you can extend sharing privileges for your own user record. However, you can't restrict access below your organization's default access levels.

You can share external user records, such as external community users and customer portal or partner portal users. You can also share an internal user record with an external user. To view and manage sharing details, click **Sharing** on the user detail page. The Sharing Detail page lists the users, groups, roles, and territories that have sharing access to the user record. On this page, you can perform these tasks.

- To show a filtered list of items, select a predefined list from the `View` drop-down list, or click **Create New View** to define your own custom views. To edit or delete any view you created, select it from the `View` drop-down list and click **Edit**.
- Grant access to the record for other users, groups, roles, or territories by clicking **Add**. This method of granting access is also known as *manual sharing* of your user records.
- Edit or delete the manual share by clicking **Edit** or **Del** next to the rule.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view user records:

- Read on user records

An administrator can disable or enable manual user record sharing for all users.

SEE ALSO:

User Sharing

Differences Between User Sharing with Manual Sharing and Sharing Sets

Grant Access to User Records

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To grant access to your own user record:

- Read on the user with whom you're sharing

You can manually grant access to your user records so that others can access them. Users inherit the same access permissions as users below them in the role hierarchy. Granting access to a user record makes the user's detail page visible to others. It also makes the user visible in lookups, list views, search, and so on.

You can share your user record manually if others cannot access it through the organization-wide defaults, sharing rules, or role hierarchy. If you gain access through more than one method, the higher level of access is maintained. High-volume portal users can be shared with other users using manual shares, but not in sharing rules.

1. From Setup, enter `Users` in the `Quick Find` box, then select **Users**. Click the name of the user you want to share.
2. On the User Detail page, click **Sharing**.
3. Click **Add**.
4. From the drop-down list, select the group, user, role, or territory to share with.
5. Choose which users have access by adding them to the Share With list.
6. Select the access level for the record you are sharing.

   Possible values are Read/Write or Read Only, depending on your organization-wide defaults for users. You can only grant a higher access level than your organization-wide default.
7. Click **Save**.
8. To change record access, on the user's Sharing Detail page, click **Edit** or **Del**.

Controlling Who Community or Portal Users Can See

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To set Community and Portal User Visibility:

- Manage Sharing

If your organization has enabled a community and has portal licenses provisioned for it, User Sharing is enabled automatically. When User Sharing is on, you can choose which other users community users can see by default. If your organization has Customer or Partner Portals, you can choose a default for them as well. Users who can see one another can interact on all the communities or portals in your organization. For example, if you would like to have a more private community, you can deselect the **Community User Visibility** checkbox and use other sharing features like sharing rules, manual shares, or portal access.

For Communities and Portals, you can choose different defaults.

Communities

The initial default is to allow community users to be seen by all other internal and external users in communities they are a member of. You can change the default to allow external users in communities to be seen only by themselves and their superiors in the role hierarchy. The setting provides Read access only and applies to all communities in your organization.

Visibility to users as a result of the **Community User Visibility** preference is not inherited through the role hierarchy. If a manager in the role hierarchy is not a member of a community, but their subordinate is, the manager does not gain access to other members of the community.If Portal User Visibility is also selected, portal users can see other portal users from the same account as well.

Portals

The initial default is to allow portal users to be seen by other portal users within the same account. You can change the default to allow external users in portals to be seen by only themselves and their superiors in the role hierarchy. The setting provides Read access only and applies to all of the portals in your organization. If Community User Visibility is also selected, users from the same community can see each other as well.

Note: Partner portal users also have access to their channel manager.

1. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
2. Click **Edit** in the Organization-Wide Defaults area.
3. Deselect the **Portal User Visibility** checkbox to allow users to be seen by only themselves and their superiors. Or select the checkbox to let portal users be seen by all other portal users within the same account.
4. For **Community User Visibility**, deselect the checkbox to allow users to be seen only by themselves and their superiors. Select the checkbox to allow community users to be seen by all other users in their communities.

   Note: This option only appears if Salesforce Communities is enabled.

5. Click **Save**.

Selecting either of these options is a quick way of overriding an organization-wide default setting of Private for external access to the User object for Community or Portal users.

Once you have set these defaults, you can selectively expand access to users.

SEE ALSO:

Set the Org-Wide Sharing Defaults for User Records

Creating User Sharing Rules

Control Standard Report Visibility

User Sharing

Control Standard Report Visibility

Show or hide standard reports that might expose data of users to whom a user doesn't have access.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To set standard report visibility:

- Manage Sharing

You can control whether users can see reports based on standard report types that can expose data of users to whom they don't have access. When User Sharing is first enabled, all reports that contain data of users to whom a viewing user doesn't have access are hidden.

1. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
2. Click **Edit** in the Organization-Wide Defaults area.
3. To allow users to view reports based on standard report types that can expose data of users to whom they don't have access, select the **Standard Report Visibility** checkbox . Or, to hide these reports, deselect this checkbox.
4. Click **Save**.

If the organization-wide default for the user object is Private and the Standard Report Visibility checkbox is selected, a viewing user can see only the names of the users that they don't have access to in the report. User details such as username and email are hidden. When you deselect the **Standard Report Visibility** checkbox, users with the "View All Users" permission can still see all reports based on standard report types. All users can also see these reports if the organization-wide default for the user object is Public Read Only.

Important: When Analytics sharing is in effect, all users in the organization get Viewer access to report and dashboard folders that are shared with them. Users who have been designated Manager or Editor on a folder, and users with additional administrative permissions, can have more access. Each user's access to folders is based on the combination of folder access and user permissions. To ensure that standard report folders are hidden as needed, remove sharing for all users from the folders. Then deselect the **View Dashboards in Public Folders** and **View Reports in Public Folders** checkboxes for the users' profiles.

SEE ALSO:

User Sharing

Report Types Support for User Sharing

Control Manual Sharing for User Records

Enable or prevent users from sharing their own user records with other users across the organization.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To enable or disable manual user record sharing:

- Manage Users

You can control whether the **Sharing** button is displayed on user detail pages. This button enables a user to grant others access to the user's own user record. You can hide or display this button for all users by following these steps.

1. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
2. Click **Edit** in the Organization-Wide Defaults area.
3. Select the **Manual User Record Sharing** checkbox to display the **Sharing** button on user detail pages, which enables users to share their records with others. Or deselect the checkbox to hide the button, which prevents users from sharing their user records with others.
4. Click **Save**.

When the organization-wide default for users is set to Public Read Only, users get read access to all other user records, can see those users in search and list views, and can interact with those users on Chatter and Communities.

Example: For example, a partner user wants to collaborate with the sales representative in Communities. If you have disabled the `Community User Visibility` checkbox in the Sharing Settings page, community users can only be seen by themselves and their superiors in the role hierarchy. You can use manual sharing to grant the partner user read access to the sales representative by using the **Sharing** button on the sales representative's user detail page. This access enables both parties to interact and collaborate in Communities.

SEE ALSO:

Controlling Who Community or Portal Users Can See

Restoring User Visibility Defaults

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Portals and communities available in: Salesforce Classic

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

USER PERMISSIONS

To restore user visibility defaults:

- Manage Sharing

User Sharing enables you to control who sees who in the organization. You can restore your defaults if you have previously used User Sharing.

To restore user visibility defaults:

1. From Setup, enter *`Sharing Settings`* in the `Quick Find` box, then select **Sharing Settings**.
2. Set the organization-wide defaults to Public Read Only for internal access and Private for external access.
3. Enable portal account user access.

   On the Sharings Settings page, select the **Portal User Visibility** checkbox. This option enables customer portal users to see other users under the same portal account. Additionally, partner portal users can see the portal account owner. If Community User Visibility is also selected, users from the same community can see each other as well.
4. Enable network member access.

   On the Sharing Settings page, select the **Community User Visibility** checkbox. This option enables community members to be seen by all other users in their communities. If Portal User Visibility is also selected, portal users can see other portal users from the same account as well.
5. Remove user sharing rules.

   On the Sharing Settings page, click **Del** next to all available user sharing rules.
6. Remove HVPU access to user records.

   On the Customer Portal Setup page, click **Del** next to all available sharing sets for HVPUs.

After user visibility is restored to the defaults, all internal users are visible to each other, portal users under the same portal account are visible to each other, and community members in the same community are visible to each other.

SEE ALSO:

Controlling Who Community or Portal Users Can See

User Sharing

Report Types Support for User Sharing

Reports based on standard report types might expose data of users to whom a user doesn't have access.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

The following report types might expose data of users to whom a viewing user doesn't have access.

- Accounts
- Account Owners
- Accounts with Assets
- Accounts with Custom Objects
- Accounts with Partners
- API Usage
- Campaigns with Opportunities
- Customizable Forecasting: Forecast History
- Customizable Forecasting: Opportunity Forecasts
- Custom Object Opportunity with Quotes Report
- Events with Invitees
- Opportunity
- Opportunity Field History
- Opportunity History
- Opportunity Trends
- Opportunities and Connections
- Opportunities with Competitors
- Opportunities with Contact Roles
- Opportunities with Contact Roles and Products
- Opportunities with Custom Objects
- Opportunities with Partners
- Opportunities with Products
- Opportunities with Products and Schedules
- Opportunities with Quotes and Quote Documents
- Opportunities with Quotes and Quote Line Items
- Opportunities with Sales Teams
- Opportunities with Sales Teams and Products
- Split Opportunities
- Split Opportunities with Products
- Split Opportunities with Products and Schedules

By default, these reports are accessible only to users who have the appropriate access. However, you can change the setting such that users without the appropriate access to the relevant users can see those reports.

Additionally, some reports may display a user's role. When a user can see a record but does not have access to the record owner, the user can see the owner's role on those reports.

SEE ALSO:

Control Standard Report Visibility

User Sharing

Differences Between User Sharing with Manual Sharing and Sharing Sets

Manual sharing and sharing sets provide access to different groups of users.

You can control who sees whom in the organization, including internal and external users, if your organization has User Sharing enabled. Manual sharing and sharing sets provide additional access beyond the organization-wide defaults and sharing rules. External users, such as high-volume portal or community users (HVPU), don't have roles and can't be used in sharing rules.

EDITIONS

Available in: Salesforce Classic

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

Example: Grant internal and non-HVPU users access to a user by creating a manual share using the Sharing button on the user detail page of that user. Grant HVPUs access to other users by creating a sharing set for your portals or communities.

The following table shows when to use manual sharing and sharing sets.

Users Getting Access

	Internal	**Non-HVPU**[1]	**HVPU**[2]
Internal	Manual Sharing	Manual Sharing	Sharing Set
Non-HVPU	Manual Sharing	Manual Sharing	Sharing Set
HVPU	Manual Sharing	Manual Sharing	Sharing Set

[1] Non-HVPU refers to an external user who is not using an HVPU profile.

[2] HVPU refers to an external user that has one of these profiles:

- Authenticated Website
- Customer Community User
- Customer Community Login User
- High Volume Customer Portal
- High Volume Portal
- Overage Authenticated Website User
- Overage High Volume Customer Portal User

SEE ALSO:

User Sharing

Share User Records

Sharing Set Overview

Sharing Considerations

Learn how sharing models give users access to records they don't own.

The sharing model is a complex relationship between role hierarchies, user permissions, sharing rules, and exceptions for certain situations. Review the following notes before setting your sharing model:

Exceptions to Role Hierarchy-based Sharing

Users can always view and edit all data owned by or shared with users below them in the role hierarchy. Exceptions to this include:

- An option on your organization-wide default allows you to ignore the hierarchies when determining access to data.
- Contacts that are not linked to an account are always private. Only the owner of the contact and administrators can view it. Contact sharing rules do not apply to private contacts.
- Notes and attachments marked as private via the `Private` checkbox are accessible only to the person who attached them and administrators.
- Events marked as private via the `Private` checkbox are accessible only by the event owner. Other users cannot see the event details when viewing the event owner's calendar. However, users with the "View All Data" or "Modify All Data" permission can see private event details in reports and searches, or when viewing other users' calendars.
- Users above a record owner in the role hierarchy can only view or edit the record owner's records if they have the "Read" or "Edit" object permission for the type of record
- Visibility to users as a result of the **Community User Visibility** preference is not inherited through the role hierarchy. If a manager in the role hierarchy is not a member of a community, but their subordinate is, the manager does not gain access to other members of the community. This only applies if Salesforce Communities is enabled in your organization.

Deleting Records

- The ability to delete individual records is controlled by administrators, the record owner, users in a role hierarchy above the record owner, and any user that has been granted "Full Access."
- If the sharing model is set to Public Read/Write/Transfer for cases or leads or Public Full Access for campaigns, any user can delete those types of records.

Adding Related Items to a Record

- You must have "Read/Write" access to a record to be able to add notes or attachments to the record.
- You must have at least "Read" access to a record to be able to add activities or other associated records to it.

Adding or Removing Sharing Access Manually

- The ability to manually extend the sharing access of individual records is controlled by administrators, the record owner, users in a role hierarchy above the record owner, and any user that has been granted "Full Access."
- Changing your sharing model deletes any manual shares your users have created.

User Permissions and Object-Level Permissions

While your sharing model controls visibility to records, user permissions and object-level permissions control what users can do to those records.

- Regardless of the sharing settings, users must have the appropriate object-level permissions. For example, if you share an account, those users can only see the account if they have the "Read" permission on accounts. Likewise, users who have the "Edit" permission on contacts may still not be able to edit contacts they do not own if they are working in a Private sharing model.
- Administrators, and users with the "View All Data" or "Modify All Data" permissions, have access to view or edit all data.

Account Sharing

- To restrict users' access to records they do not own that are associated with accounts they do own, set the appropriate access level on the role. For example, you can restrict a user's access to opportunities they do not own yet are associated with accounts they do own using the `Opportunity Access` option.
- Regardless of the organization-wide defaults, users can, at a minimum, view the accounts in their territories. Also, users can be granted access to view and edit the contacts, opportunities, and cases associated with their territories' accounts.

Apex Sharing

The organization-wide default settings can't be changed from private to public for a custom object if Apex code uses the sharing entries associated with that object. For example, if Apex code retrieves the users and groups who have sharing access on a custom object Invoice__c (represented as `Invoice__share` in the code), you can't change the object's organization-wide sharing setting from private to public.

Campaign Sharing

- In Professional, Enterprise, Unlimited, Performance, and Developer Editions, designate all users as Marketing Users when enabling campaign sharing. This simplifies administration and troubleshooting because access can be controlled using sharing and profiles.
- To segment visibility between business units while maintaining existing behavior within a business unit:
  1. Set the campaign organization-wide default to Private.
  2. Create a sharing rule to grant marketing users Public Full Access to all campaigns owned by users within their business unit.
  3. Create a sharing rule to grant all non-marketing users in a business unit Read Only access to all campaigns owned by users in their business unit.
- When a single user, such as a regional marketing manager, owns multiple campaigns and needs to segment visibility between business units, share campaigns individually instead of using sharing rules. Sharing rules apply to all campaigns owned by a user and do not allow segmenting visibility.
- Create all campaign sharing rules prior to changing your organization-wide default to reduce the affect the change has on your users.
- To share all campaigns in your organization with a group of users or a specific role, create a sharing rule that applies to campaigns owned by members of the "Entire Organization" public group.
- Minimize the number of sharing rules you need to create by using the "Roles and Subordinates" option instead of choosing a specific role.
- If campaign hierarchy statistics are added to the page layout, a user can see aggregate data for a parent campaign and all the campaigns below it in the hierarchy regardless of whether that user has sharing rights to a particular campaign within the hierarchy. Therefore, consider your organization's campaign sharing settings when enabling campaign hierarchy statistics. If you do not want

users to see aggregate hierarchy data, remove any or all of the campaign hierarchy statistics fields from the Campaign Hierarchy related list. These fields will still be available for reporting purposes.

- If the sharing model is set to Public Full Access for campaigns, any user can delete those types of records.

Campaign Member Sharing

Campaign member sharing is controlled by campaign sharing rules. Users that can see a campaign can also see associated campaign members.

Contact Sharing

See: Business Contact Sharing for Orgs That Use Person Accounts

Price Book Sharing

- Sharing on price books controls whether users can add the price book and its products to opportunities.
- User permissions control whether users can view, create, edit, and delete price books.

SEE ALSO:

Sharing Rules

Sharing Settings

Who Has Access to Account Records?

A user may have access to an account from:

- Record Ownership
- Implicit access from an associated child record such as a case, contact, or opportunity
- Organization-wide sharing defaults
- Role hierarchy
- Sharing rules
- Manual sharing
- Account team or territory

To find out why a user have access to the record, click the **Sharing** button on the account detail page to see a list of users who have access and for which reasons. Click **Expand List** to see all users who have access.

The following users don't show up in the list even if they may have access:

- All users, if the organization-wide defaults are set to Public Read Only or Public Read/Write
- High-volume portal users

Note: If the **Sharing** button does not appear, the organization-wide sharing defaults may have been set to Controlled by Parent or Public Read. Otherwise, only the record owner, an administrator, or a user above the owner in the role hierarchy can see the Sharing Detail page.

Table 2: Troubleshooting guideline for user access to a record

Access Type	Description
Record owner	The record owner always gets access to his or her own record.
Implicit access	Corresponds to the “Associated record owner or sharing” entry in the Reason column of the Sharing Detail page. The user may have access to a child record of an account (opportunity, case, or contact), which grants them Read access on that account. You cannot overwrite this access. For example, if the user has access to a case record, he or she has implicit Read access to the parent account record.
Organization-wide sharing default	Check if the defaults for the account object are set to Private. If it is, the user may have gained access via other methods listed here. It must be set to Private if at least one of your users should not see a record.
Role hierarchy	The user may have inherited Read access from a subordinate in the role hierarchy. You can’t override this behavior for non-custom objects. If the user who has access is on a different branch of the hierarchy from the account owner, check the sharing rules, account teams, and account territory.
Sharing rules	The user may have gotten access because he or she has been included in a relevant sharing rule. If the sharing rule uses public groups (or other categories such as roles) to grant access, check your public groups to see if the user has been included in the group.
Manual shares	The user may have gotten access through the **Sharing** button of the record. Only the record owner, an administrator, or a user above the owner in the role hierarchy can create or remove a manual share on the record.
Account Teams and Territory	The user may have been added to an Account Team by the account owner, an administrator, a user above the owner in the role hierarchy, or an account team member. If your organization uses territory management, check if the user who has access is higher in the territory hierarchy than the account owner. Managers gain the same access as their subordinates. Additionally, if the user is a member of Group A, which is a member of Group B, he or she gets access to all accounts shared to Group B, at the same level of access as members of Group B.

SEE ALSO:

Control Who Sees What

Resolving Insufficient Privileges Errors

Viewing Sharing Overrides

When you select an object in the Sharing Settings page, the page includes a Sharing Overrides related list, which shows any profiles that ignore sharing settings for that object.

To view the Sharing Overrides list, from Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**. Next, select an object from the Manage Sharing Settings For list.

For each profile, the list specifies the permissions that allow it to override sharing settings. The "View All Data" and "Modify All Data" permissions override sharing settings for all objects in the organization, while the object permissions "View All" and "Modify All" override sharing settings for the named object.

Note: The Sharing Overrides list doesn't show permissions granted through permission sets, which may also override sharing settings for an object.

To override sharing settings for specific objects, you can create or edit permission sets or profiles and enable the "View All" and "Modify All" object permissions. These permissions provide access to all records associated with an object across the organization, regardless of the sharing settings. Before setting these permissions, compare the different ways to control data access.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view sharing overrides:
- View Setup and Configuration

SEE ALSO:

Profiles

Recalculate Sharing Rules

When you make changes to groups, roles, and territories, sharing rules are reevaluated to add or remove access as necessary.

Changes could include adding or removing individual users from a group, role, or territory, changing which role a particular role reports to, changing which territory a particular territory is subordinate to, or adding or removing a group from within another group.

Note: Use the Recalculate buttons on the Sharing Rules related lists only if sharing rule updates have failed or are not working as expected.

To manually recalculate an object's sharing rules:

1. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.
2. In the Sharing Rules related list for the object you want, click **Recalculate**.
3. If you want to monitor the progress of a recalculation, from Setup, enter `Background Jobs` in the `Quick Find` box, then select **Background Jobs**.

Note: The **Recalculate** button is disabled when group membership or sharing rule calculations are deferred. Sharing rules for related objects are automatically recalculated. For example, account sharing rules are recalculated when opportunity sharing rules are recalculated since the opportunity records are in a master-detail relationship on account records.

When sharing is recalculated, Salesforce also runs all Apex sharing recalculations. During sharing rule recalculation, related object sharing rules are calculated as well. You receive an email that notifies you when the recalculation is completed. For example, when recalculating sharing rule for opportunities, account sharing rules are recalculated as well since opportunity is a detail of an account object.

Automatic sharing rule calculation is enabled by default. You can defer sharing rule calculation by suspending and resuming at your discretion.

SEE ALSO:

Sharing Rules

Defer Sharing Calculations

Monitoring Background Jobs

Asynchronous Parallel Recalculation of Sharing Rules

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Account and contact sharing rules are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Account territory, case, lead, opportunity, order sharing rules, and custom object sharing rules are available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Campaign sharing rules are available in **Professional** Edition for an additional cost, and **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To recalculate sharing rules:

- Manage Sharing

Asynchronous Parallel Recalculation of Org-Wide Defaults

When you update an org-wide default, recalculation is now processed asynchronously and in parallel. This change provides optimal efficiency of server resources and guards against site operations such as patches and server restarts.

You receive an email notification when the recalculation is completed. Consider the following guidelines when updating your org-wide defaults.

- While recalculation is in progress, you can't create, update, or delete sharing rules and org-wide defaults for that object. However, you can make changes to the org-wide default and sharing rules for another object.
- Updating the org-wide default on an account or its children—cases, contacts, and opportunities—disables further org-wide default and sharing rule updates on them. For example, when you update the opportunity org-wide default and recalculation is in progress, you can't update the org-wide default or sharing rules for accounts, contacts, opportunities, and cases.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

SEE ALSO:

Recalculate Sharing Rules

Asynchronous Parallel Recalculation of Sharing Rules

Asynchronous Parallel Recalculation of Sharing Rules

Speed up sharing rule recalculation by running it asynchronously and in parallel.

When you create, update, or delete sharing rules, the resulting recalculation is now processed asynchronously and in parallel. The recalculation is run in parallel and asynchronously in the background, which speeds up the process and provides better resilience to site operations such as patches and server restarts. You'll receive an email notification upon completion. Before the recalculation is completed, you can't run other sharing operations such as creating a sharing rule or updating the organization-wide defaults.

If the number of impacted records from an owner-based sharing rule insert or update is less than 25,000, recalculation runs synchronously and you won't receive an email notification when it's completed. Owner-based sharing rule inserts and updates impacting less than 25,000 records are not available on the Background Jobs page.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Parallel sharing rule recalculation is also run in these cases.

- Click the Recalculate button for the sharing rules on the Sharing Settings page
- Recalculate your sharing rules on the Defer sharing page

You can monitor the progress of your parallel recalculation on the Background Jobs page or view your recent sharing operations on the View Setup Audit Trail page.

Recalculation of sharing rules maintains implicit sharing between accounts and child records. In the Background Jobs page, these processes corresponds to these job sub types:, **Account — Extra Parent Access Removal** and **Account — Parent Access Grant**. Additionally, deleting a sharing rule corresponds to the job sub type **Object — Access Cleanup**, denoting that irrelevant share rows are removed.

Note: For an in-depth look at record access, see *Designing Record Access for Enterprise Scale*.

SEE ALSO:

Monitoring Background Jobs

Recalculate Sharing Rules

Built-in Sharing Behavior

Asynchronous Deletion of Obsolete Shares

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Obsolete shares are removed asynchronously, so admins don't have to wait for shares to be deleted to perform other operations.

Note: To enable asynchronous deletion of obsolete shares, contact Salesforce Customer Support. This feature is not enabled by default.

Many sharing operations have an immediate impact on the visibility of records within the system. For example, deleting a group revokes the access granted to that group via sharing rules or manual shares.

Members of the following groups lose access to records immediately. Users above these members in the role hierarchy also lose access to the records.

- Public groups
- Queues
- Roles
- Territories

When deleting a group, the shares to the group become obsolete. Obsolete shares are deleted asynchronously during off-peak hours to minimize your waiting time during this operation.

When deactivating a user, the user's manually assigned shares and their team shares are deleted asynchronously. Until the obsolete shares are deleted, users higher in the role hierarchy retain access to the records associated with these shares. If that visibility is a concern, remove the record access granted to the user before deactivating the account. All other user-related share types are deleted immediately when the user is deactivated.

Defer Sharing Calculations

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Performing a large number of configuration changes can lead to very long sharing rule evaluations or timeouts. To avoid these issues, an administrator can suspend these calculations and resume calculations during an organization's maintenance period.

Note: The defer sharing calculation feature isn't enabled by default. To enable it for your organization, contact Salesforce.

Deferring sharing calculation is ideal if you make a large number of changes to roles, territories, groups, users, portal account ownership, or public groups participating in sharing rules, and want to suspend the automatic sharing calculation to a later time.

Group membership and sharing rule calculation are enabled by default.

If	You can
Group membership and sharing rule calculation are enabled	- Suspend, update, and resume group membership calculation. This suspends sharing rule calculation and requires a full recalculation of sharing rules. - Suspend, update, and resume sharing rule calculation.
Group membership calculation is enabled and sharing rule calculation is suspended	Suspend, update, and, resume group membership calculation.
Group membership calculation is suspended and sharing rule calculation is enabled	Suspend, update, resume, and recalculate sharing rule calculation.

To suspend or resume group membership calculation, see Manage Group Membership Calculations.

To suspend, resume, or recalculate sharing rule calculation, see Deferring Sharing Rule Calculations.

SEE ALSO:

Recalculate Sharing Rules

Manage Group Membership Calculations

If you are making changes to groups that affect a lot of records, you may want to suspend automatic group membership calculation and resume at a later time. Note that you might experience sharing inconsistencies in your records if you don't resume calculation.

When you make changes to roles, territories, groups, or users, or change ownership of portal accounts, group membership is automatically recalculated to add or remove access as necessary. Changes can include adding or removing a user from a group or changing a role to allow access to different sets of reports.

To suspend or resume group membership calculation:

1. From Setup, enter `Defer Sharing Calculations` in the `Quick Find` box, then select **Defer Sharing Calculations**.
2. In the Group Membership Calculations related list, click **Suspend**.

   Note: If sharing rule calculations are enabled, suspending group membership calculations also suspends sharing rule calculations. Resuming group membership calculations also requires full sharing rule recalculation.

3. Make your changes to roles, territories, groups, users, or portal account ownership.
4. To enable group membership calculation, click **Resume**.

SEE ALSO:

Defer Sharing Calculations

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To defer (suspend and resume) sharing calculations:

- Manage Users

  AND

  Manage Sharing Calculation Deferral

Deferring Sharing Rule Calculations

Note: The defer sharing calculation feature isn't enabled by default. To enable it for your organization, contact Salesforce.

To suspend, resume, or recalculate sharing rule calculation:

1. From Setup, enter `Defer Sharing Calculations` in the `Quick Find` box, then select **Defer Sharing Calculations**.
2. In the Sharing Rule Calculations related list, click **Suspend**.
3. Make changes to sharing rules, roles, territories, or public groups participating in sharing rules.

   Note: Any changes to sharing rules require a full recalculation.

   To enable sharing rule calculation, click **Resume**.
4. To manually recalculate sharing rules, click **Recalculate**.

Consider deferring your sharing calculations before performing massive updates to sharing rules. When sharing is recalculated, Salesforce also runs all Apex sharing recalculations.

SEE ALSO:

Manage Group Membership Calculations

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Account and contact sharing rules are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Account territory, case, lead, and opportunity, sharing rules are available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Campaign sharing rules are available in **Professional** Edition for an additional cost, and **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Custom object sharing rules are available in: **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions.

USER PERMISSIONS

To defer (suspend and resume) and recalculate sharing rules:

- Manage Users

  AND

  Manage Sharing Calculation Deferral

Object-Specific Share Locks

When you create, edit, or delete a sharing rule, recalculation runs to update record access in your org. This operation can take some time if you have many users and records. Object-specific share locks feature enables you to make changes to a sharing rule for other objects simultaneously, depending on the objects affected by the sharing rules, sharing rule type, and target groups or roles of the affected users.

Without object-specific share locks, you can't submit simultaneous sharing changes until recalculation across all objects is complete. If you are enabling object-specific share locks, consider the following changes in your org.

EDITIONS

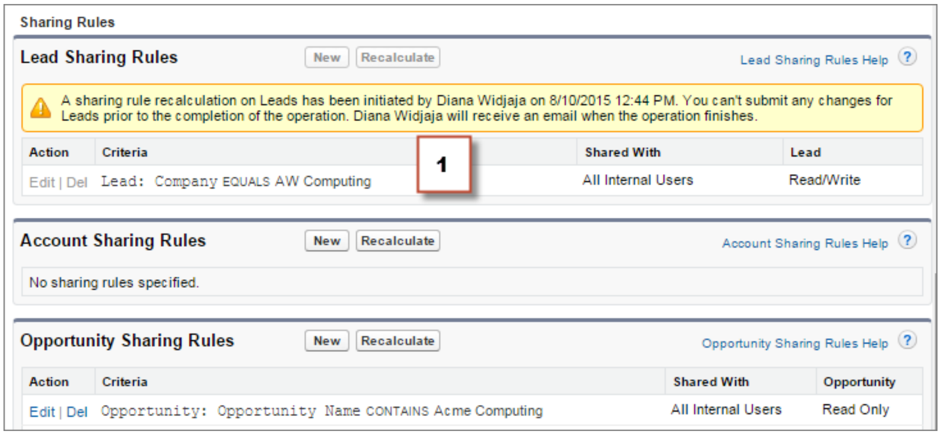
Available in: Salesforce Classic and Lightning Experience

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

Criteria-based and ownership-based sharing rules

Recalculation is run if a sharing rule has changed or when you click the **Recalculate** button on the Sharing Settings page. Clicking this button locks sharing rules for that object (1), but you can still make changes to sharing rules for another object.

Note: Use the Recalculate buttons on the Sharing Rules related lists only if sharing rule updates have failed or are not working as expected.


Sharing Rules

Lead Sharing Rules

A sharing rule recalculation on Leads has been initiated by Diana Widjaja on 8/10/2015 12:44 PM. You can't submit any changes for Leads prior to the completion of the operation. Diana Widjaja will receive an email when the operation finishes.

Action	Criteria	Shared With	Lead
Edit | Del	`Lead: Company` EQUALS AW Computing	All Internal Users	Read/Write

Account Sharing Rules

No sharing rules specified.

Opportunity Sharing Rules

Action	Criteria	Shared With	Opportunity
Edit | Del	`Opportunity: Opportunity Name` CONTAINS Acme Computing	All Internal Users	Read Only

When recalculation for an ownership-based sharing rule is in progress, you can't create, edit, or delete ownership-based sharing rules for that object targeting the same group of users. For example, let's say you're creating an ownership-based lead sharing rule targeting the All Internal Users group. While recalculation is in progress, you can create another ownership-based sharing rule for leads targeting any other public group except the All Internal Users group. You can create, update, or delete ownership-based sharing rules for leads targeting all internal users only after the recalculation finishes. You receive an email notification when the recalculation is complete.

When recalculation for a criteria-based sharing rule is in progress, you can't edit or delete that rule. But you can create, edit, or delete any other criteria-based or ownership-based sharing rule for that object regardless of the target group of users.

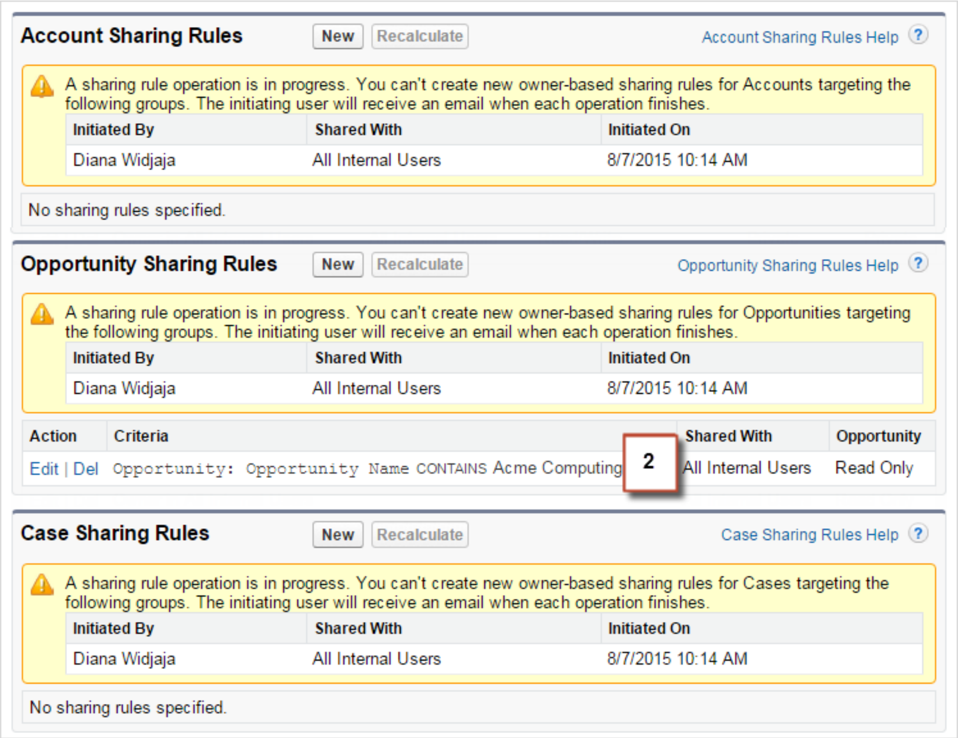
Note: You can't modify the org-wide defaults when a sharing rule recalculation for any object is in progress. Similarly, you can't modify sharing rules when recalculation for an org-wide default update is in progress.

Account, cases, contacts, and opportunities

Sharing rules can affect accounts and the associated account children—cases, contacts, and opportunities—so they are locked together to ensure that recalculation runs properly. For example, creating or editing an account sharing rule prevents you from creating or editing a case, contact, or opportunity sharing rule. Similarly, creating or editing an opportunity sharing rule prevents you from creating or editing a case, contact, or account sharing rule before recalculation is complete. Locks are not shared across objects, except across accounts and associated account children.

Note: Clicking the **Recalculate** button for any of these four objects' sharing rules prevents anyone from making changes to sharing rules for those objects until recalculation finishes.

In the following example, an ownership-based account sharing rule has been deleted and recalculation is in progress. Although you can't create, edit, or delete another ownership-based sharing rule for any of these objects, you can make changes to a criteria-based sharing rule (2) for those objects.



Account Sharing Rules

A sharing rule operation is in progress. You can't create new owner-based sharing rules for Accounts targeting the following groups. The initiating user will receive an email when each operation finishes.

Initiated By	Shared With	Initiated On
Diana Widjaja	All Internal Users	8/7/2015 10:14 AM

No sharing rules specified.

Opportunity Sharing Rules

A sharing rule operation is in progress. You can't create new owner-based sharing rules for Opportunities targeting the following groups. The initiating user will receive an email when each operation finishes.

Initiated By	Shared With	Initiated On
Diana Widjaja	All Internal Users	8/7/2015 10:14 AM

Action	Criteria	Shared With	Opportunity
Edit | Del	Opportunity: Opportunity Name CONTAINS Acme Computing	All Internal Users	Read Only

Case Sharing Rules

A sharing rule operation is in progress. You can't create new owner-based sharing rules for Cases targeting the following groups. The initiating user will receive an email when each operation finishes.

Initiated By	Shared With	Initiated On
Diana Widjaja	All Internal Users	8/7/2015 10:14 AM

No sharing rules specified.

SEE ALSO:

- Sharing Rules
- Recalculate Sharing Rules
- Defer Sharing Calculations

Built-in Sharing Behavior

Salesforce provides implicit sharing between accounts and child records (opportunities, cases, and contacts), and for various groups of portal users.

EDITIONS

Available in: Salesforce Classic

Sharing for accounts and contacts is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Sharing for cases and opportunities is available in **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Sharing between accounts and child records

- **Access to a parent account**—If you have access to an account's child record, you have implicit Read Only access to that account.
- **Access to child records**—If you have access to a parent account, you have access to the associated child records. The account owner's role determines the level of access to child records.

Sharing behavior for portal users

- **Account and case access**—An account's portal user has Read Only access to the parent account and to all of the account's contacts.
- **Management access to data owned by Service Cloud portal users**—Since Service Cloud portal users don't have roles, portal account owners can't access their data via the role hierarchy. To grant them access to this data, you can add account owners to the portal's share group where the Service Cloud portal users are working. This step provides access to all data owned by Service Cloud portal users in that portal.
- **Case access**—If a portal user is a contact on a case, then the user has Read Only access on the case.

Group membership operations and sharing recalculation

Simple operations such as changing a user's role, moving a role to another branch in the hierarchy, or changing a portal account's owner can trigger a recalculation of sharing rules. Salesforce must check access to user's data for people who are above the user's new or old role in the hierarchy, and either add or remove shares to any affected records.

Note: These sharing behaviors simplify administration for data access but can make mass inserts and mass updates slow. For best practices on designing record access in a large organization, see *Designing Record Access for Enterprise Scale*.

SEE ALSO:

Control Who Sees What

Resolving Insufficient Privileges Errors

If you can't access a record or perform a task, like run a report, you most likely don't have the required permission or sharing setting.

EDITIONS

Available in: Salesforce Classic

Available in: **All Editions**

You see the Insufficient Privileges error, if you don't have the right access on different levels. For example, your profile prevents you from accessing the account object, or your role prevents you from accessing a case record. You also see an Insufficient Privileges error when you click a link to a record or a Visualforce page tab to which you don't have access.

Record owners can resolve most cases by using the Sharing button on the record detail page, which enables them to share the record to another user. Administrators can also resolve this issue using the API, such as querying the UserRecordAccess object to check a user's access to a set of records. For more information, see the *SOAP API Developer's Guide*.

If these tools can't help you resolve the issue, an administrator can try to diagnose it with this troubleshooting flow.

- Resolve object-level access errors by reviewing the user profiles and permission sets.
- Resolve record-level access errors by reviewing the sharing settings, such as organization-wide defaults and sharing rules.
- Resolve process-level errors by reviewing validation rules and Apex triggers.

It's a good idea for an administrator to log in to the application using your login to help you resolve an issue. You can grant administrators access for a specified duration.

Note: Watch this video series to understand how to grant users the access they need. ▶ Who Sees What

Resolve Permission and Object-Level Access Errors

EDITIONS

Available in: Salesforce Classic

Available in: **All Editions**

USER PERMISSIONS

To view profiles and permission sets:

- View Setup and Configuration

To edit object permissions:

- Manage Profiles and Permission Sets

  AND

  Customize Application

Missing or incorrect object and user permissions can cause Insufficient Privileges errors. You can troubleshoot this type of error by checking profile and permission sets.

Generally, the best method for investigating object and permission access issues is through the API. However, you can use the following steps to investigate via point-and-click tools.

1. Verify the object permissions in the user's profile.

   Object permissions, configured on profiles and permission sets, determine which objects a user can read, create, edit, or delete.

   a. On the user detail page, click the user's profile.

   b. On the profile overview page, go to **Object Settings** or **Object Permissions**.

      Note the permissions for the object. If the user is trying to view an account, check that the "Read" permission for the account and contact objects on the user profile is enabled.

      If the user is trying to run a report, check that the user has "Read" permission on an object that the report references.

2. Verify the user permissions in one of the following ways, depending on your profile user interface.

   - From the enhanced profile user interface, review the permissions in the App Permissions and System Permissions sections.
   - From the original profile user interface, review the permissions under Administrative Permissions and General User Permissions.

   Note the relevant user permissions. For example, if the user is trying to send an email to a lead, check that the "Send Email" permission is enabled.

3. Verify the permissions in the user's permission sets.

   a. On the user detail page, scroll to the Permission Set Assignments related list and click each permission set.

   b. On the permission set overview page, click Object Settings and review the assigned object permissions.

   c. Review the user permissions in the App Permissions and System Permissions sections.

   d. Repeat these steps for each permission set assigned to the user.

4. If needed, assign the necessary permission using a permission set or by updating the profile. Permission sets provide access on an individual basis. Assign permissions on the user profile *only* if all users of this profile require access. Be sure you're aware of your organization's security policy and act accordingly.

SEE ALSO:

Resolving Insufficient Privileges Errors

Permission Sets

User Permissions and Access

Profiles

Resolve Record-Level Access Errors

Your sharing settings, such as roles or sharing rules, can cause Insufficient Privileges errors.

To verify if the error is at record-level, follow these steps. You can also use the API to query a user's access to a set of records or use the Sharing button on the record detail page.

EDITIONS

Available in: Salesforce Classic

Available in: **All Editions**

USER PERMISSIONS

To create or edit sharing rules:
- Manage Sharing

To set up teams:
- Customize Application

To manage territories:
- Manage Territories

1. If your organization uses roles, check the user's role in relation to the record owner.

   For example, users can delete records only if they are the record owner, higher in the role hierarchy than the record owner, or the administrator. Similarly, users always have read access to records whose owners are below them in the role hierarchy, unless **Grant Access Using Hierarchies** is deselected (custom objects only).

   a. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.

      Verify the role of the user and the role of the user who owns the record. A user can't delete or merge accounts owned by someone in an unrelated role hierarchy, even if the user has the appropriate permissions on the objects.

2. Review your sharing rules.

   Check that the user is included in the sharing rules.

   a. From Setup, enter `Sharing Settings` in the `Quick Find` box, then select **Sharing Settings**.

   b. Check the public group (or other categories such as roles or queues) and verify that the user is included in that sharing rule.

3. Verify your sales teams.

   If your organization uses teams for accounts, opportunities, or cases, check that you didn't miss the user when you set up the teams. Review your teams to determine if the user is supposed to have access through a team.

   a. From Setup, enter the team that you want to check, such as `Account Teams`, in the `Quick Find` box, then select the team.

      Add the user to the team, if appropriate.

4. Review your manual shares.

   If the user had access via a manual share but then lost this access because

   - The record owner changed, causing the manual share to be automatically dropped
   - The record owner, an administrator, or a user above the owner in the role hierarchy removed the manual share using the **Sharing** button on the record detail page

   a. On the record detail page, click **Sharing**.

      The Sharing Detail page shows the users, groups, roles, and territories that have access to the record.

   b. If the user must gain access via a manual share, create a manual share by clicking **Add**.

5. Review your territories.

   If your organization is using territories, check that

   - The user included in the territories

- The record is under the correct territory where the user is a member.

SEE ALSO:

Resolving Insufficient Privileges Errors
User Role Hierarchy
Sharing Rules

Resolve Process-Level Access Errors

Validation rules can cause Insufficient Privileges errors.

To resolve Insufficient Privileges errors, you typically determine if misconfigured permission sets, profiles, or sharing settings are causing the errors. Another option is to review your organization’s validation rules.

1. Review your validation rules.

   A validation rule can prevent the user from completing a task, such as transferring a case record after it’s closed.

2. From your object management settings, find the object that you want to check, and then scroll down to Validation Rules.
3. Verify that none of the validation rules are causing the error or fix the validation rule.

SEE ALSO:

Resolving Insufficient Privileges Errors
Define Validation Rules

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **All Editions**

USER PERMISSIONS

To view and change validation rules:

- View Setup and Configuration

  AND

  Customize Application

To view and define Apex triggers:

- Author Apex

Managing Folders

A *folder* is a place where you can store reports, dashboards, documents, or email templates. Folders can be public, hidden, or shared, and can be set to read-only or read/write. You control who has access to its contents based on roles, permissions, public groups, and license types. You can make a folder available to your entire organization, or make it private so that only the owner has access.

- To access document folders, click the **Documents** tab.
- To access email template folders, from Setup, enter `Email Templates` in the `Quick Find` box, then select **Email Templates**.

To create a folder, click **Create New Folder**.

To edit a folder, click **Edit** next to the folder name. Alternatively, select a folder name from the Folder drop-down list and click **Edit**.

Note: You can modify the contents of a folder only if the folder access level is set to read/write. Only users with the “Manage Public Documents” or “Manage Public Templates” permission can delete or change a read-only folder. Regardless of permissions or folder settings, users can’t edit unfiled or personal folders. Users with the “Manage Reports in Public Folders” permission can edit all reports in public folders but not reports in other users’ personal folders.

SEE ALSO:

Creating and Editing Folders

Deleting Folders

Filing Items in Folders

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Report folders not available in: **Contact Manager**, **Group**, and **Personal** Editions

USER PERMISSIONS

To create, edit, or delete public document folders:

- Manage Public Documents

To create, edit, and delete public email template folders:

- Manage Public Templates (in Salesforce Classic only)

To create, edit, and delete public report folders:

- Manage Reports in Public Folders

To create, edit, and delete public dashboard folders:

- Manage Dashboards AND View All Data

Creating and Editing Folders

Click **Create New Folder** or **Edit** from most pages that list folders.

1. Enter a `Folder Label`. The label is used to refer to the folder on user interface pages.
2. If you have the "Customize Application" permission, enter a unique name to be used by the API and managed packages.
3. Choose a `Public Folder Access` option. Select read/write if you want users to be able to change the folder contents. A read-only folder can be visible to users but they can't change its contents.
4. Select an unfiled report, dashboard, or template and click **Add** to store it in the new folder. Skip this step for document folders.
5. Choose a folder visibility option:
   - `This folder is accessible by all users, including portal users` gives folder access to all users in your organization, including portal users.
   - `This folder is accessible by all users, except for portal users` gives folder access to all users in your organization, but denies access to portal users. This option is only available for report and dashboard folders in organizations with a partner portal or Customer Portal enabled. If you don't have a portal, you won't see it.
   - `This folder is hidden from all users` makes the folder private.
   - `This folder is accessible only by the following users` allows you to grant access to a desired set of users:
     a. Choose "Public Groups", "Roles," "Roles and Subordinates," "Roles, Internal and Portal Subordinates" (if you have portals enabled), "Territories," or "Territories and Subordinates" from the `Search` drop-down list. The choices vary by Edition and whether your organization has territory management.

        Note: When you share a folder with a group, managers of the group members have no access to the folder unless those managers are also members of the group.

     b. If the `Available for Sharing` list does not immediately display the desired value, enter search criteria and click **Find**.
     c. Select the desired value from the `Available for Sharing` list and click **Add** to move the value to the `Shared To` list.

   Note: You can use enhanced folder sharing to give your users more detailed levels of access to reports folders and dashboard folders. For more information, see Turn On Enhanced Folder Sharing for Reports and Dashboards and Share a Report or Dashboard Folder in Salesforce Classic.

6. Click **Save**.

SEE ALSO:

Managing Folders

EDITIONS

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

Report folders not available in: **Contact Manager**, **Essentials**, **Group**, and **Personal** Editions

Document folder restriction is available in: **Enterprise**, **Performance**, and **Unlimited** Editions

USER PERMISSIONS

To create, edit, or delete public document folders:
- Manage Public Documents

To create, edit, and delete public email template folders:
- Manage Public Templates (in Salesforce Classic only)

To create, edit, and delete public report folders:
- Manage Reports in Public Folders

To create, edit, and delete public dashboard folders:
- Manage Dashboards AND View All Data

Deleting Folders

You can only delete folders that are empty. Before you begin, remove all the documents, dashboards, templates, or reports from the folder you would like to delete.

1. Click **Edit** next to the folder name from any page that lists folders. On the Reports tab, click ▼ then **Edit** in the Folders pane.
2. Click **Delete** or ▼ then **Delete**.
3. Click **OK** to confirm.

SEE ALSO:

Managing Folders

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Report folders not available in: **Contact Manager**, **Group**, and **Personal** Editions

USER PERMISSIONS

To create, edit, or delete public document folders:

- Manage Public Documents

To create, edit, and delete public email template folders:

- Manage Public Templates (in Salesforce Classic only)

To create, edit, and delete public report folders:

- Manage Reports in Public Folders

To create, edit, and delete public dashboard folders:

- Manage Dashboards AND View All Data

Filing Items in Folders

To move a document, dashboard, report, or email template to a different folder:

1. Select the item to be stored in a folder.
2. Click **Edit Properties**.
3. Choose another folder.
4. Click **Save**.

Just like report folders contain reports and email template folders contain email templates, document folders can only contain documents. To store an attachment in a document folder, save the attachment to your computer and upload it to the document library.

Note: Email templates that are used by Web-to-Case, Web-to-Lead, assignment rules, or escalation rules must be marked as "Available for Use."

SEE ALSO:

Managing Folders

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Report folders not available in: **Contact Manager**, **Group**, and **Personal** Editions

USER PERMISSIONS

To create, edit, or delete public document folders:
- Manage Public Documents

To create, edit, and delete public email template folders:
- Manage Public Templates (in Salesforce Classic only)

To create, edit, and delete public report folders:
- Manage Reports in Public Folders

To create, edit, and delete public dashboard folders:
- Manage Dashboards AND View All Data

Import Data Into Salesforce

You can import up to 50,000 records into Salesforce.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small popup windows, while the Data Import Wizard opens in a full browser with dataimporter.app at the end of the URL. From Setup, enter *`Data Import Wizard`* in the `Quick Find` box, then select **Data Import Wizard**. The options you see depend on your permissions.

You can import data from ACT!, Outlook, and any program that can save data in comma-delimited text format (.csv), such as Excel or GoldMine.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Your edition determines the types of objects you can import.

Note: If commas aren't appropriate for your locale, use a tab or other delimiter. Specify your delimiter in Data Loader Settings (**Settings** | **Settings**).

The number of records you can import depends on your permissions and the type of data you're importing. You can import as many records as allowed, as long as you don't exceed the overall data storage limits for your org.

Which records can be imported?

Type of record	Import record limit	Users permissions needed	Learn more
Business accounts and contacts owned by you	50,000 at a time via the Data Import Wizard	Import Personal Contacts	What Is Imported for Business Accounts and Contacts?
Business accounts and contacts owned by other users	50,000 at a time	Modify All Data	What Is Imported for Business Accounts and Contacts?
Person accounts owned by you	50,000 at a time	Create on accounts AND Edit on accounts AND Import Personal Contacts	What Is Imported for Person Accounts?
Person accounts owned by other users	50,000 at a time	Create on accounts AND Edit on accounts and contacts AND Modify All Data	What Is Imported for Person Accounts?
Leads	50,000 at a time	Import Leads	What Is Imported for Leads?
Campaign members	50,000 at a time	Depends on what's being imported: • Campaign member statuses • Existing contacts • Existing leads • Existing person accounts • New contacts • New leads	What's Imported for Campaign Members? Who can import campaign members?
Custom objects	50,000 at a time	Import Custom Objects AND Create on the custom object AND Edit on the custom object	What Is Imported for Custom Objects?
Solutions	50,000 at a time	Import Solutions	What Is Imported for Solutions?

Which records can be imported?

Type of record	Import record limit	Users permissions needed	Learn more
Assets Cases Campaigns Contracts Documents Opportunities Products	You can't import these records via the Data Import Wizard.		

For information on field accessibility and how different field type values are imported, see Notes on Importing Data on page 403.

Note: Relationship group members can't be imported.

SEE ALSO:

- Data Import Wizard
- Choosing a Method for Importing Data
- Undoing an Import
- What permissions do I need to import records?

Choosing a Method for Importing Data

Learn about your options for importing data into Salesforce.

Tool	Editions supported	Number of records you can import or export	Import	Export	Internal or external to Salesforce	Additional information
Data Import Wizard (unified)	All except Personal and Database.com Editions	Up to 50,000	Yes	No	Internal	An in-browser wizard that imports your org's accounts, contacts, leads, solutions, campaign members, and custom objects. Read more.
Data Loader	Enterprise, Unlimited, Performance, Developer, and	Between 5,000 and 5 million	Yes	Yes	External	Data Loader is an application for the bulk import or export of data. Use it to insert, update, delete, or

Tool	Editions supported	Number of records you can import or export	Import	Export	Internal or external to Salesforce	Additional information
	Database.com Editions					export Salesforce records. Read more.

SEE ALSO:

Data Import Wizard

Import Data Into Salesforce

What Is Imported for Business Accounts and Contacts?

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Org import not available in: **Personal** Edition, **Database.com**

The Data Import Wizard allows you to match records in multiple ways to prevent duplicates. You can match contacts by Salesforce ID, name, email, or external ID. You can match business accounts by Salesforce ID, external ID, or by name and site. Matching by Salesforce ID is inclusive of both contacts and business accounts. If you match one by Salesforce ID, the other is also matched by Salesforce ID.

Matching by Name and Site

If you are matching contacts by name and business accounts by name and site (which are the recommended options), the Data Import Wizard creates a business account for each unique business account name and site in the import file. It also creates a separate contact for each contact name listed in the file. The contacts are then associated with the appropriate business accounts.

If the business account or contact exists in the system, and you have read/write access to the record, the wizard adds your import data to the existing data in Salesforce.

Matching by Salesforce ID

You can also choose to match contacts and business accounts by Salesforce ID. With this option, the Salesforce ID is the criteria for de-duplication. That is, if you are matching by ID and a record in your source file has the same ID as a record in Salesforce, that record is updated in Salesforce. Record IDs are case-sensitive and must match exactly.

Matching by External ID

An external ID is a custom field that has the External ID attribute, meaning that it contains unique record identifiers from a system outside of Salesforce. When you select this option, the Data Import Wizard detects existing records in Salesforce with external IDs that match those values in the import file.

- This operation isn't case-sensitive. For example, "ABC" is matched with "abc". However, if the external ID field also has the case-sensitive Unique attribute, uppercase and lowercase letters aren't considered identical.
- External IDs can be of type text, number, email, or auto-number. If the external ID type is auto-number, it isn't available for matching, but it can be used to look up the parent record if it contains the external ID.
- External ID values should be standardized before performing the import to prevent unintended matches.
- Multiple records with the same External ID within a file aren't uploaded.
- Multiple external ID fields can be used to find matching records in Salesforce when using the Data Import Wizard.

Overwriting Existing Account Values

The wizard never overwrites your existing business account fields unless you select **Overwrite existing account values**. This option lets you insert or update existing business account fields with new data. However, you cannot use this option to update existing field data with blank values. If you do not select this option, the wizard updates the empty business account fields, but does not touch fields with data.

If you do not have read/write access to an existing business account or contact, the wizards create a new business account or contact owned by you. In addition, the wizards create new business accounts and contacts based on specific fields in your import file.

In Professional, Enterprise, Unlimited, Performance, and Developer Edition orgs, the import wizards can also import new business account and contact notes. The wizards do not import notes that are exact duplicates of existing contact or business account notes.

To import account or contact notes, make the owner field in the imported file the Salesforce ID.

SEE ALSO:

Data Import Wizard

Choosing a Method for Importing Data

Import Data Into Salesforce

What Is Imported for Person Accounts?

The Data Import Wizard prevents creating duplicate person accounts by matching records according to one of the following fields: `Account Name`, `Salesforce ID`, `Email`, or an external ID field. In your import file, include a column for the field that you're using for record matching.

Note: Your administrator could have renamed "person account" to another term. If so, the Data Import Wizard refers to the new name.

EDITIONS

Data Import Wizard available in both Salesforce Classic and Lightning Experience

Data Import Wizard available in **All** Editions except Database.com

Person accounts available in: both Salesforce Classic and Lightning Experience

Person accounts available in **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Matching by Name

When you select this option, the Data Import Wizard detects existing records in Salesforce that have the same name. This type of matching is not case-sensitive. For example, names that begin with a capital letter are matched with the same name that begins with a lowercase letter. If necessary, scan and standardize your record names before performing the import to prevent unintended matches.

Matching by Salesforce ID

A Salesforce ID is a system-generated, case-sensitive string of 15 or 18 letters and numbers that uniquely identifies each Salesforce record. When you select this option, the Data Import Wizard detects existing records in Salesforce that have the same Salesforce ID. You can obtain Salesforce IDs by running reports that include the ID field of the record.

Matching by Email

With this option, records in your import file are matched with existing records in Salesforce according to the exact value in the Email field.

Matching by External ID

An external ID is a custom field that has the External ID attribute, meaning that it contains unique record identifiers from a system outside of Salesforce. When you select this option, the Data Import Wizard detects existing records in Salesforce with external IDs that match those values in the import file.

- This operation isn't case-sensitive. For example, "ABC" is matched with "abc". However, if the external ID field also has the case-sensitive Unique attribute, uppercase and lowercase letters aren't considered identical.
- External IDs can be of type text, number, email, or auto-number. If the external ID type is auto-number, it isn't available for matching, but it can be used to look up the parent record if it contains the external ID.
- External ID values should be standardized before performing the import to prevent unintended matches.
- Multiple records with the same External ID within a file aren't uploaded.
- Multiple external ID fields can be used to find matching records in Salesforce when using the Data Import Wizard.

Ignoring or Updating Matching Records

When the Data Import Wizard detects existing records in Salesforce that match according to your chosen field, you can choose one of these actions.

- **Add new records**—If records in your file are new and don't match existing records, insert them into Salesforce. Ignore records in your file that match existing records, and do nothing to the existing records.
- **Update existing records**—If records in your file match existing records, update the existing records. Ignore records in your file that don't match existing records, and don't insert them as new records.
- **Add new and update existing records**—If records in your file are new and don't match existing records, insert them into Salesforce. If records in your file match existing records, update the existing records.

What Is Imported for Leads?

You can import data into standard lead fields and custom lead fields, even if a field is hidden or read only in your page layout or field-level security settings for leads.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Importing Leads with Matching Types

You can choose whether to match leads in your import file with existing leads in Salesforce. Leads can be matched according to the following types: Salesforce ID, name, email, or external ID. Choosing a matching type sets the criteria for avoiding duplicate leads. For example, if you're matching by email and a lead in your source file has the same email as a lead in Salesforce, that lead is updated in Salesforce. If you aren't matching by email and a lead in your source file has the same email as a lead in Salesforce, a lead is created.

Importing Leads Without Matching Types

If you choose a matching type of "None" in the Data Import Wizard, for each lead in your import file, the Data Import Wizard creates a lead in Salesforce. You can merge leads after they are imported.

Matching by Name

When you select this option, the Data Import Wizard detects existing records in Salesforce that have the same name. This type of matching is not case-sensitive. For example, names that begin with a capital letter are matched with the same name that begins with a lowercase letter. If necessary, scan and standardize your record names before performing the import to prevent unintended matches.

Matching by Email

With this option, records in your import file are matched with existing records in Salesforce according to the exact value in the Email field.

Matching by Salesforce ID

A Salesforce ID is a system-generated, case-sensitive string of 15 or 18 letters and numbers that uniquely identifies each Salesforce record. When you select this option, the Data Import Wizard detects existing records in Salesforce that have the same Salesforce ID. You can obtain Salesforce IDs by running reports that include the ID field of the record.

Matching by External ID

An external ID is a custom field that has the External ID attribute, meaning that it contains unique record identifiers from a system outside of Salesforce. When you select this option, the Data Import Wizard detects existing records in Salesforce with external IDs that match those values in the import file.

- This operation isn't case-sensitive. For example, "ABC" is matched with "abc". However, if the external ID field also has the case-sensitive Unique attribute, uppercase and lowercase letters aren't considered identical.
- External IDs can be of type text, number, email, or auto-number. If the external ID type is auto-number, it isn't available for matching, but it can be used to look up the parent record if it contains the external ID.
- External ID values should be standardized before performing the import to prevent unintended matches.
- Multiple records with the same External ID within a file aren't uploaded.
- Multiple external ID fields can be used to find matching records in Salesforce when using the Data Import Wizard.

SEE ALSO:

Data Import Wizard

Choosing a Method for Importing Data

What's Imported for Campaign Members?

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

You can use the Data Import Wizard to update the statuses of campaign members.

You can also import campaign members. For each contact, lead, or person account in your import file, the Data Import Wizard:

- Imports the record
- Associates the record with the specified campaign, making the contact, lead, or person account a campaign member
- Inserts a Member Status value for the campaign member

If your import file has duplicate records, the Data Import Wizard doesn't merge them. If an imported record matches an existing record, the Data Import Wizard doesn't merge the duplicate data into one record.

Matching by External ID

An external ID is a custom field that has the External ID attribute, meaning that it contains unique record identifiers from a system outside of Salesforce. When you select this option, the Data Import Wizard detects existing records in Salesforce with external IDs that match those values in the import file.

- This operation isn't case-sensitive. For example, "ABC" is matched with "abc". However, if the external ID field also has the case-sensitive Unique attribute, uppercase and lowercase letters aren't considered identical.
- External IDs can be of type text, number, email, or auto-number. If the external ID type is auto-number, it isn't available for matching, but it can be used to look up the parent record if it contains the external ID.
- External ID values should be standardized before performing the import to prevent unintended matches.
- Multiple records with the same External ID within a file aren't uploaded.
- Multiple external ID fields can be used to find matching records in Salesforce when using the Data Import Wizard.

SEE ALSO:

Import Campaign Members

Data Import Wizard

What Is Imported for Custom Objects?

The Data Import Wizard prevents creating duplicate records by matching records according to one of the following fields: custom object name, Salesforce ID, or external ID. In your import file, include a column for the field that you are using for record matching.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Custom object import available in: **Contact Manager**,**Essentials**, **Group**, **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To import custom object data via the Data Import Wizard:

- Import Custom Objects

  AND

  Create on the custom object

  AND

  Edit on the custom object

Matching by Name

When you select this option, the Data Import Wizard detects existing records in Salesforce that have the same name. This type of matching is not case-sensitive. For example, names that begin with a capital letter are matched with the same name that begins with a lowercase letter. If necessary, scan and standardize your record names before performing the import to prevent unintended matches.

Matching by Salesforce ID

A Salesforce ID is a system-generated, case-sensitive string of 15 or 18 letters and numbers that uniquely identifies each Salesforce record. When you select this option, the Data Import Wizard detects existing records in Salesforce that have the same Salesforce ID. You can obtain Salesforce IDs by running reports that include the ID field of the record.

Matching by External ID

An external ID is a custom field that has the External ID attribute, meaning that it contains unique record identifiers from a system outside of Salesforce. When you select this option, the Data Import Wizard detects existing records in Salesforce with external IDs that match those values in the import file.

- This operation isn't case-sensitive. For example, "ABC" is matched with "abc". However, if the external ID field also has the case-sensitive Unique attribute, uppercase and lowercase letters aren't considered identical.
- External IDs can be of type text, number, email, or auto-number. If the external ID type is auto-number, it isn't available for matching, but it can be used to look up the parent record if it contains the external ID.
- External ID values should be standardized before performing the import to prevent unintended matches.
- Multiple records with the same External ID within a file aren't uploaded.

- Multiple external ID fields can be used to find matching records in Salesforce when using the Data Import Wizard.

SEE ALSO:

Data Import Wizard

Choosing a Method for Importing Data

What Is Imported for Solutions?

The Data Import Wizard prevents creating duplicate records by matching records according to one of the following fields: solution title, Salesforce ID, or external ID. In your import file, include a column for the field that you are using for record matching.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To import solutions:
- Import Solutions

Matching by Solution Title

When you select this option, the import wizard detects existing solutions in Salesforce that have the same title. This type of matching isn't case-sensitive. For example, titles that begin with a capital letter are matched with the same title that begins with a lowercase letter. If necessary, scan and standardize your solution titles before performing the import to prevent unintended matches.

Matching by Salesforce ID

A Salesforce ID is a system-generated, case-sensitive string of 15 or 18 letters and numbers that uniquely identifies each Salesforce record. When you select this option, the Data Import Wizard detects existing records in Salesforce that have the same Salesforce ID. You can obtain Salesforce IDs by running reports that include the ID field of the record.

Matching by External ID

An external ID is a custom field that has the External ID attribute, meaning that it contains unique record identifiers from a system outside of Salesforce. When you select this option, the Data Import Wizard detects existing records in Salesforce with external IDs that match those values in the import file.

- This operation isn't case-sensitive. For example, "ABC" is matched with "abc". However, if the external ID field also has the case-sensitive Unique attribute, uppercase and lowercase letters aren't considered identical.
- External IDs can be of type text, number, email, or auto-number. If the external ID type is auto-number, it isn't available for matching, but it can be used to look up the parent record if it contains the external ID.
- External ID values should be standardized before performing the import to prevent unintended matches.
- Multiple records with the same External ID within a file aren't uploaded.
- Multiple external ID fields can be used to find matching records in Salesforce when using the Data Import Wizard.

SEE ALSO:

Data Import Wizard

Choosing a Method for Importing Data

Notes on Importing Data

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Your edition determines the types of objects you can import.

- **Field Accessibility**—You can import values into a field only if you have read and edit access. User permissions, page layout assignments, and field-level security settings determine field access.

  Field-level security is available in Professional, Enterprise, Unlimited, Performance, and Developer Editions.

- **New Values for Picklists and Multi-Select Picklists**—If you import a picklist value that doesn't match an existing picklist value:
  - For an unrestricted picklist, the Data Import Wizard uses the value that's in the import file.
  - For a restricted picklist, the Data Import Wizard uses the picklist's default value.

- **Multi-Select Picklists**—To import multiple values into a multi-select picklist, separate the values by a semicolon in your import file.

  You can import up to 100 values at a time in a multi-select picklist field. If you have more than 100 values in your import file for any one record, the import wizard leaves the field blank in that record.

- **Checkboxes**—To import data into a checkbox field, use 1 for checked values and 0 for unchecked values.
- **Default Values**—For picklist, multi-select picklist, and checkbox fields, if you do not map the field in the import wizard, the default value for the field, if any, is automatically inserted into the new or updated record.
- **Date/Time Fields**—Ensure that the format of any date/time fields you are importing matches how they display in Salesforce per your locale setting.
- **Formula Fields**—Formula fields cannot accept imported data because they are read only.
- **Field Validation Rules**—Salesforce runs validation rules on records before they are imported. Records that fail validation aren't imported. Consider deactivating the appropriate validation rules before running an import if they affect the records you are importing.
- **Geolocation Custom Fields**—To import a geolocation custom field using the Data Import Wizard, supply two values: a latitude and a longitude. Import both values in one field, separated by a semicolon. If you enter only one value, it is imported as the latitude, and the longitude is interpreted as 0. If you supply more than two values, the import fails for the entire row.
- **Currency Fields**—If you have currency data in your CSV file, format your values for your locale. For example, if you're in the U.S. locale, use periods for decimals and commas for thousand markers. Using the incorrect currency format could change your imported values.

SEE ALSO:

Data Import Wizard

Choosing a Method for Importing Data

Import Data Into Salesforce

Importing Multiple Currencies

If your organization has set up the ability to use multiple currencies, you can import amounts in different currencies.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Organization Import

When importing accounts, contacts, custom objects, leads, or solutions for your organization, you can specify the currency type for amount fields using the `Currency ISO Code` column in your import file. The following rules apply.

- **Entering currency codes** - Enter a currency code in the `Currency ISO Code` column in your import file. Currency codes are three letter codes that follow an international standard. For example, USD is the currency code for U.S. dollars. From Setup, enter *`Manage Currencies`* in the `Quick Find` box, then select **Manage Currencies** to see a list of valid codes for your organization.
- **Updating the currency code** - When updating the currency code but not the currency amount for accounts and contacts, the amount isn't converted to the corresponding number in the new currency.
- **Entering inactive currencies** - If you enter an inactive currency in your import file, your personal currency is used instead. However, amounts aren't modified. For example, if your file has AUD 100 for 100 Australian dollars but AUD is an inactive currency for your organization, it's imported as USD 100, assuming your personal currency is U.S. dollars.
- **Omitting the Currency ISO Code column** - When creating records via importing, if you don't use the `Currency ISO Code` column or fail to map it, your personal currency is used. For example, if your file has 100 and your personal currency is U.S. dollars (currency code = USD), it's imported as USD 100.

  When updating existing records via importing, if you don't use the `Currency ISO Code` column or fail to map it, any amounts are interpreted as having the currency of the record. For example, if your file has 100 for a record that has a currency of EUR (the currency code for euros), this amount is interpreted as EUR 100.

SEE ALSO:

Data Import Wizard

Create Export Files for Import Wizards

Before you can import data into Salesforce, use your existing software to create a data export file.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

An export file contains all the information you want to import.

Your export file can contain a mixture of new records and updates to existing records. You'll choose how records are matched to avoid duplication. For example, you can choose to match accounts and contacts by name or by email address. If you choose to match by email address, then the contact already in Salesforce will be updated if a record in your imported data has the same email address. However, if records have the same name but different email addresses, the records will remain separate.

1. Use your existing software to create a data export file.
   - Exporting from ACT!
   - Exporting from LinkedIn®
   - Exporting from Outlook
   - Exporting from Other Data Sources

- Exporting from Salesforce

2. Review data you will import to ensure that it is more up-to-date than what is already in Salesforce. Your Salesforce data will be replaced with data from your import file, even if it is out of date.
3. Compare your data fields with the Salesforce fields you can import into, and verify that your data will be mapped into the appropriate Salesforce fields. See Prepare Your Data for Import on page 407.
4. If you are the administrator and are importing for multiple users, combine export data from multiple sources into a single comma delimited text file (.csv) using Excel.

Note: When importing records from multiple users, your export file must include a `Record Owner` field for all new records which must contain the full usernames or first and last names of existing, active users. Existing record owners will not be changed; new records will be assigned to the user listed in the `Record Owner` field. For example, records that should be owned by Joe Smith in your organization must have that user's username ("jsmith@acme.com") or first and last names (for example, "Joe Smith", or "Smith Joe" for Asian locales). For lead imports, you can also specify the name of a lead queue.

When importing leads, you can alternatively use a lead assignment rule to specify the owners of the imported data, instead of using a `Record Owner` field.

Exporting from ACT!

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

ACT! allows you to export contact data in a text-delimited format which can then be imported. To export contact data from ACT! (versions 4.0 or 2000):

1. Launch ACT! and open your database.
2. Select **File** > **Data Exchange** > **Export...**.
3. Select the file type **Text-Delimited**.
4. Choose a file name and location for the exported data and click **Next**.
5. Select **Contact records only**.
6. Click the **Options...** button.
7. Select **Comma** for the field separator character.

Note: If commas aren't appropriate for your locale, use a tab or other delimiter. Specify your delimiter in Data Loader Settings (**Settings** | **Settings**).

8. Select **Yes, export field names** and click **OK**.
9. Click **Next**.
10. Select **All Records** and then click **Next**.
11. Leave the export field order list alone, and click **Finish**.

SEE ALSO:

Default Field Mapping for ACT!

Create Export Files for Import Wizards

Exporting from LinkedIn®

You can export contact data from LinkedIn in a text-delimited format, which you can then import.

- Open `www.linkedin.com/addressBookExport` and follow the steps on the page using the **Microsoft Outlook (.CSV file)** option.

Exporting from Outlook

Export data directly from Microsoft® Outlook® in a CSV (comma-separated values) format. Then import that data into Salesforce.

EDITIONS

Available in: Salesforce Classic

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

1. In Outlook, navigate to the export feature.
2. Choose **Comma Separated Values (Windows)** and click **Next**.

   Note: If commas aren't appropriate for your locale, use a tab or other delimiter. Specify your delimiter in Data Loader Settings (**Settings** | **Settings**).

3. Select the folder containing the contacts you want to export, and click **Next**.
4. Choose a file name for the exported data and click **Next**.
5. Click **Finish**.

SEE ALSO:

Default Field Mapping for Outlook

Create Export Files for Import Wizards

Exporting from Other Data Sources

You can import data into the system from any other application that can create a CSV (comma-separated values) file.

1. Save your data source as a CSV file.

   Note: If commas aren't appropriate for your locale, use a tab or other delimiter. Specify your delimiter in Data Loader Settings (**Settings** | **Settings**).

2. Ensure your file includes only one name per field. The system cannot accept more than one name per field.
3. Ensure your file separates names and titles into two fields. The system cannot accept fields containing both names and titles.
4. Ensure your file includes only one phone number per field.

SEE ALSO:

Field Mapping for Other Data Sources and Organization Import

Create Export Files for Import Wizards

Exporting from Salesforce

You can export account, campaign member, contact, custom object, lead, or solution reports from Salesforce to create an import file. Include the `Account ID`, `Campaign Member ID`, `Contact ID`, `Custom Object ID`, `Lead ID`, or `Solution ID` value for each respective record in your report. These ID fields are unique Salesforce identifiers and are used to accurately match your data with existing Salesforce records.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

To create an import file with these ID fields, first export the data from Salesforce.

1. Run an account, campaign member, contact, custom object, lead, or solution report in Salesforce.

   Include the respective ID field and any other fields that are required for the import.

2. Export the report to Excel.

Note: Remember that Salesforce record IDs are case-sensitive. Don't manually change Salesforce IDs in your import file.

SEE ALSO:

Create Export Files for Import Wizards

Videos: Data Import How-To Series

Prepare Your Data for Import

After exporting your data from Salesforce or your existing application, prepare your data before importing it.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Note: If your data has information in fields that do not match any standard fields, your admin can create custom fields for that data before import.

Preparing Contacts

Use Excel® to label the columns in your import file as specified in Field Mapping for Other Data Sources and Organization Import on page 414.

Preparing Person Accounts

When importing person accounts, use the field labels in Salesforce as the column labels in your import file.

Preparing Org Business Accounts and Contacts

When importing business accounts and contacts for your org, you must use Excel® to label the columns in your import file as specified in Field Mapping for Other Data Sources and Organization Import on page 414.

Preparing Org Leads

When importing general leads or leads for campaigns, use the import file labels specified in Field Mapping for Importing Leads on page 418.

Preparing Custom Objects

When importing a custom object, use the field labels shown on the custom object detail page in Salesforce as the column labels in your import file.

Preparing Campaign Members

When importing campaign members, use the field labels in Salesforce as the column labels in your import file.

Preparing Solutions

When importing solutions, use the field labels in Salesforce as the column labels in your import file.

You can enter HTML into the solutions you plan to import into Salesforce. However, unless your org has enabled HTML solutions, HTML tags will display in the solutions after they are imported.

For security purposes, Salesforce automatically filters all HTML solutions for potentially malicious HTML. If potentially malicious HTML is detected in an HTML solution, the potentially malicious HTML is either removed or transformed into text for users who view the HTML solution. Users can't notice when potentially malicious HTML is removed from an HTML solution.

You can import solutions written in HTML format into Salesforce. However, for security purposes, only the HTML tags listed below are allowed. The content of any HTML tags not listed below is removed when saved in HTML solutions. Furthermore, the content of all `<script>` and `<iframe>` tags, as well as all JavaScript, is removed when saved in HTML solutions. Cascading Style Sheets (CSS) are not supported in HTML solutions.

The following HTML tags are allowed in HTML solutions imported into Salesforce:

- `<a>`
- `<abbr>`
- `<acronym>`
- `<address>`
- `<b>`
- `<bdo>`
- `<big>`
- `<blockquote>`
- `<br>`
- `<caption>`
- `<cite>`
- `<code>`
- `<col>`
- `<colgroup>`
- `<dd>`
- `<del>`
- `<dfn>`
- `<div>`
- `<dl>`
- `<dt>`
- `<em>`
- `<font>`
- `<h1>`
- `<h2>`
- `<h3>`
- `<h4>`
- `<h5>`
- `<h6>`
- `<hr>`
- `<i>`
- `<img>`
- `<ins>`
- `<kbd>`
- `<li>`
- `<ol>`
- `<p>`
- `<pre>`
- `<q>`
- `<samp>`
- `<small>`
- `<span>`
- `<strike>`
- `<strong>`
- `<sub>`
- `<sup>`
- `<table>`
- `<tbody>`
- `<td>`
- `<tfoot>`
- `<th>`
- `<thead>`
- `<tr>`
- `<tt>`
- `<ul>`
- `<var>`

Within the above tags, you can include the following attributes:

- `alt`
- `background`
- `face`
- `height`
- `size`
- `src`

border	href	style
class	name	target
colspan	rowspan	width

The above attributes, which can include a URL, are limited to URLs that begin with the following:

- http:
- https:
- file:
- ftp:
- mailto:
- #
- / for relative links

SEE ALSO:

Default Field Mapping for ACT!

Default Field Mapping for Outlook

Create Export Files for Import Wizards

Default Field Mapping for ACT!

This table details how ACT! fields map to Salesforce account and contact import fields during an individual data import.

Note: If an ACT! record contains more than one contact for the same company, the import wizard creates multiple contacts for one account.

ACT! Field	Import Field
Address 1	Contact: Mailing Address and Account: Billing Address
Address 2	Contact: Mailing Address and Account: Billing Address
Address 3	Contact: Mailing Address and Account: Billing Address
Alt Phone	Contact: Other Phone
Alt Phone Ext.	Contact: Other Phone Ext.
Assistant	Contact: Assistant's Name
Asst. Phone	Contact: Asst. Phone

EDITIONS

Available in: Salesforce Classic

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

ACT! Field	Import Field
Asst. Phone Ext.	Contact: Asst. Phone Ext.
City	Contact: Mailing City and Account: Billing City
Company	Account: Name
Contact	Contact: Full Name
Country	Contact: Mailing Country and Account: Billing Country
Department	Contact: Department
E-mail Login (The import wizard verifies this is a valid email address in the form: jsmith@acme.com)	Contact: Email
Fax	Contact: Fax and Account: Fax
Fax Ext.	Contact: Business Fax Ext.
First Name	Contact: First Name
Home Address 1	Contact: Other Address 1
Home Address 2	Contact: Other Address 2
Home Address 3	Contact: Other Address 3
Home City	Contact: Other City
Home Country	Contact: Other Country
Home Phone	Contact: Home Phone
Home State	Contact: Other State
Home Zip	Contact: Other Postal Code
ID/Status	Account: Type
Last Name	Contact: Last Name
Mobile Phone	Contact: Mobile Phone
Note	Does not import
Phone	Contact: Phone and Account: Phone
Phone Ext.	Contact: Business Phone Ext.

ACT! Field	Import Field
Referred By	Contact: Lead Source
Revenue	Account: Annual Revenue
State	Contact: Mailing State and Account: Billing State
Ticker Symbol	Account: Ticker Symbol
Title	Contact: Title
Web Site	Account: Website
Zip	Contact: Mailing Postal Code Account: Billing Postal Code
2nd Contact	2nd Contact: Name
2nd Phone	2nd Contact: Phone
2nd Phone Ext.	2nd Contact: Phone Ext.
2nd Title	2nd Contact: Title
3rd Contact	3rd Contact: Name
3rd Phone	3rd Contact: Phone
3rd Phone Ext.	3rd Contact: Phone Ext.
3rd Title	3rd Contact: Title
2nd Last Reach, 3rd Last Reach, Asst. Title, Last Attempt, Last Meeting, Last Reach, Last Results, Letter Date, Pager, Spouse, User 1-15	Contact: Note or Account: Note (In Professional, Enterprise, Unlimited, Performance, and Developer Edition organizations, you specify which fields import into a single contact or account note; separate notes are not created for each ACT! field.)

SEE ALSO:

- Exporting from ACT!
- Prepare Your Data for Import

Default Field Mapping for Outlook

This table details how Outlook fields map to Salesforce account and contact import fields during an individual data import.

EDITIONS

Available in: Salesforce Classic

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

Outlook Field	Import Field
`Assistant's Name`	Contact: `Assistant's Name`
`Assistant's Phone`	Contact: `Asst Phone`
`Birthday`	Contact: `Birthdate`
`Business City`	Contact: `Mailing City` and Account: `Billing City`
`Business Country`	Contact: `Mailing Country` and Account: `Billing Country`
`Business Fax`	Contact: `Fax` and Account: `Fax`
`Business Phone`	Contact: `Phone`
`Business Postal Code`	Contact: `Mailing Postal Code` Account: `Billing Postal Code`
`Business Street`	Contact: `Mailing Address` and Account: `Billing Address`
`Business Street 2`	Contact: `Mailing Address` and Account: `Billing Address`
`Business Street 3`	Contact: `Mailing Address` and Account: `Billing Address`
`Company`	Account: `Account Name` and Contact: `Account`
`Company Main Phone`	Account: `Phone`
`Department`	Contact: `Department`
`E-mail` (The import wizard verifies this is a valid email address in the form: jsmith@acme.com)	Contact: `Email`
`First Name`	Contact: `First Name`
`Home City`	Contact: `Other City`

Outlook Field	Import Field
Home Country	Contact: Other Country
Home Phone	Contact: Home Phone
Home Postal Code	Contact: Other Postal Code
Home Street	Contact: Other Address
Home Street 2	Contact: Other Address
Home Street 3	Contact: Other Address
Job Title	Contact: Title
Last Name	Contact: Last Name
Manager's Name	Contact: Reports To (In addition, if the name in this field does not match an existing contact, a new contact is created with the manager's name.)
Mobile Phone	Contact: Mobile Phone
Notes	Contact: Description
Other Phone	Contact: Other Phone
Referred By	Contact: Lead Source
Title	Contact: Salutation
Web Page	Account: Website
Account, Anniversary, Billing Information, Business Phone 2, Callback, Car Phone, Categories, Children, Directory Server, E-mail 2, E-mail 3, Government ID Number, Hobby, Home Fax, Home Phone 2, Internet Free/Busy Address, ISDN, Keywords, Language, Location, Middle Name, Mileage, Office Location, Organizational ID Number, Other City, Other Country, Other Fax, Other Postal Code, Other State, Other Street, Other Street 2, Other Street 3, Pager, PO Box, Primary Phone, Profession, Radio Phone, Spouse, Suffix, Telex, TTY/TDD Phone, User 1, User 2, User 3, User 4	Contact: Note or Account: Note (In Professional, Enterprise, Unlimited, Performance, and Developer Edition organizations, you specify which fields import into a single contact or account note; separate notes are not created for each Outlook field.)

SEE ALSO:

- Exporting from Outlook
- Prepare Your Data for Import

Field Mapping for Other Data Sources and Organization Import

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Organization import not available in: **Personal** Edition, **Database.com**

If you are importing accounts and contacts for an organization, or importing individual data from sources other than Outlook or ACT!, the Import Wizards map the fields as correctly as possible. You must fine-tune the mapping before completing the import. Before importing your data, Salesforce recommends that you use Excel to label the columns in your import file with the labels listed below. Field length limits for each object are listed in the Salesforce Field Reference Guide.

Note: The default mappings listed below are offered as a guide for importing; they do not ensure 100% accuracy in mapping your data. **You must fine-tune the mapping in the Import Wizards.** Remember that you can map the same field multiple times if necessary—for example, for the account and contact address fields.

Common Fields for Contacts and Accounts

Label for Your Import File	Salesforce Field
`Record Owner` (Note: For individual imports, this field is not necessary, since all data you import is automatically owned by you. In addition, when importing records by Salesforce record ID, this field is ignored.)	Contact: `Contact Owner` and Account: `Account Owner`
`Currency ISO Code` (Note: You can use this field only for organization imports in organizations that use multiple currencies. For more information, see Importing Multiple Currencies on page 404.)	Contact: `Contact Currency` and Account: `Account Currency`

Contact Fields

Label for Your Import File	Salesforce Field
`Assistant`	Contact: `Assistant`
`Asst. Phone`	Contact: `Asst. Phone`
`Asst. Phone Ext.`	Appended to Contact: `Asst. Phone`
`Birthdate`	Contact: `Birthdate`
`Business Fax`	Contact: `Fax`
`Business Fax Ext.`	Appended to Contact: `Fax`
`Business Phone`	Contact: `Phone`
`Business Phone Ext.`	Appended to Contact: `Phone`
`Contact Description`	Contact: `Description`

Contact Fields

Label for Your Import File	Salesforce Field
Contact Full Name *or* First Name & Last Name (Note: When importing contact names, use either Contact Full Name or First Name and Last Name, but not both.)	Contact: First Name and Contact: Last Name
Contact ID (Note: Record IDs are case-sensitive and should not be changed.)	Contact: Contact ID
Contact Note	Creates a note attached to the contact
Department	Contact: Department
E-mail Address (Note: The import wizard verifies this is a valid email address in the form: jsmith@acme.com.)	Contact: Email
Email Opt Out (Note: Use "1" to indicate that user opts out; use "0" to indicate that user wants emails.)	Contact: Email Opt Out
Home Phone	Contact: Home Phone
Home Phone Ext.	Appended to Contact: Home Phone
Lead Source	Contact: Lead Source
Mailing City	Contact: Mailing City
Mailing Country	Contact: Mailing Country
Mailing Postal Code	Contact: Mailing Address Zip/Postal Code
Mailing State	Contact: Mailing State/Province
Mailing Street 1	Contact: Mailing Address
Mailing Street 2	Contact: Mailing Address
Mailing Street 3	Contact: Mailing Address
Mobile Phone	Contact: Mobile
Mobile Phone Ext.	Appended to Contact: Mobile
Other City	Contact: Other City
Other Country	Contact: Other Country
Other Phone	Contact: Other Phone

Contact Fields

Label for Your Import File	Salesforce Field
Other Phone Ext.	Appended to Contact: Other Phone
Other Postal Code	Contact: Other Address Zip/Postal Code
Other State	Contact: Other State/Province
Other Street 1	Contact: Other Address
Other Street 2	Contact: Other Address
Other Street 3	Contact: Other Address
Reports To (Note: If the import wizard cannot find a contact that matches the name in this field, it will create a new contact using this value as the Contact: First Name & Last Name.)	Contact: Reports To
Salutation	Prefixed to Contact: First Name
Title	Contact: Title
2nd Contact	Split into Contact: First Name & Last Name for a second contact for the account
2nd Phone	Contact: Phone for a second contact for the account
2nd Phone Ext.	Appended to Contact: Phone for a second contact for the account
2nd Title	Contact: Title for a second contact for the account
3rd Contact	Split into Contact: First Name & Last Name for a third contact for the account
3rd Phone	Contact: Phone for a third contact for the account
3rd Phone Ext.	Appended to Contact: Phone for a third contact for the account
3rd Title	Contact: Title for a third contact for the account

Account Fields

Label for Your Import File	Salesforce Field
Account Description	Account: Description
Account Division (Note: You do not need to specify this field if you choose to assign the division via the drop-down list on Step 1 of the import wizard. If you do not map this field or use the division drop-down list, the division is set to the record owner's default division for each record.)	Account: Account Division
Account Fax	Account: Fax

Account Fields

Label for Your Import File	Salesforce Field
Account Fax Ext.	Appended to Account: Fax
Account ID (Note: Record IDs are case-sensitive and should not be changed.)	Account: Account ID
Account Name	Account: Account Name and Contact: Account
Account Note	Creates a note attached to the account
Account Number	Account: Account Number
Account Phone	Account: Phone
Account Phone Ext.	Appended to Account: Phone
Account Site	Account: Account Site
Account Type	Account: Type
Billing City	Account: Billing City
Billing Country	Account: Billing Country
Billing Postal Code	Account: Billing Zip/Postal Code
Billing State	Account: Billing State/Province
Billing Street 1	Account: Billing Address
Billing Street 2	Account: Billing Address
Billing Street 3	Account: Billing Address
Employees	Account: Employees
Industry	Account: Industry
Ownership	Account: Ownership
Parent Account (Note: If the import wizard cannot find an account that matches the parent account name, it will create a new account using this value as the Account Name.)	Account: Parent Account
Parent Account Site (Note: Indicates the site value of Parent Account.)	Account: Account Site (Note: Maps to the Account Site field in the parent account.)
Rating	Account: Rating
Revenue	Account: Annual Revenue
Shipping City	Account: Shipping City

Account Fields

Label for Your Import File	Salesforce Field
`Shipping Country`	Account: `Shipping Country`
`Shipping Postal Code`	Account: `Shipping Zip/Postal Code`
`Shipping State`	Account: `Shipping State/Province`
`Shipping Street 1`	Account: `Shipping Address`
`Shipping Street 2`	Account: `Shipping Address`
`Shipping Street 3`	Account: `Shipping Address`
`SIC Code`	Account: `SIC Code`
`Ticker Symbol`	Account: `Ticker Symbol`
`Website`	Account: `Website`

Note: If you include record types in your import file, the Import Wizard uses the record owner's default record type when creating new records. For existing records, the Import Wizard does not update the record type field.

SEE ALSO:

Prepare Your Data for Import

Field Mapping for Importing Leads

To improve the accuracy of your import, label the columns in your import file to match the Salesforce Lead fields. When you import the leads, the Data Import Wizard maps the fields in your import file

Note: The following default mappings aren't always 100% accurate in mapping your data. Check the import and fine-tune the mapping in the Data Import Wizard as necessary.

Import File Label	Salesforce Lead Field
Annual Revenue	Annual Revenue
City	City
Company	Company
Country	Country
Currency ISO Code Note: Use this field only for orgs that use multiple currencies; see Importing Multiple Currencies on page 404.	Lead Currency
Description	Description

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Import File Label	Salesforce Lead Field
Email The Data Import Wizard verifies email addresses in the form of jsmith@acme.com.	Email
Email Opt Out Use “1” to indicate that the user opts out. Use “0” to indicate that the user wants emails.	Email Opt Out
No. of Employees	No. of Employees
Fax	Fax
Full Name or First Name & Last Name (Note: When importing lead names, use either Full Name or First Name and Last Name, but not both.)	First Name and Last Name
Industry	Industry
Lead Division Note: Do not specify this field if you assign the division using the dropdown list in Step 1 of the Data Import Wizard. If you do not map this field or use the division dropdown list, the division is set to the record owner’s default division for each record.	Lead Division
Lead ID Note: Record IDs are case-sensitive and must not be changed.	Lead ID
Lead Source Note: Do not specify this field if you assign the same lead source to all leads on the first page of the Data Import Wizard. The Lead Source dropdown lists all active lead source picklist values.	Lead Source
Lead Status	Lead Status
Mobile Phone	Mobile
Phone	Phone
Postal Code	Postal Code
Rating	Rating
Record Owner Note: You do not need this field if you assign ownership using a lead assignment rule. When you import records by Salesforce record ID, this field is ignored.	Lead Owner

Import File Label	Salesforce Lead Field
Salutation	Added to beginning of First Name
State	State
Status	Status (in the Campaign History related list of a lead)
Street 1	Address
Street 2	Address
Street 3	Address
Title	Title
Website	Website

If you include record types in this list, the Data Import Wizard uses the record owner's default record type when creating new records. For existing records, the Data Import Wizard does not update the record type field.

If you use assignment rules, the Data Import Wizard uses the new owner's default record type when creating new records. When the assignment rules assign the record to a queue, the queue owner's default record type is used.

SEE ALSO:

Prepare Your Data for Import

Data Import Wizard

The Data Import Wizard makes it easy to import data for many standard Salesforce objects, including accounts, contacts, leads, solutions, campaign members, and person accounts. You can also import data for custom objects. You can import up to 50,000 records at a time.

Salesforce recommends that you test a small file first to make sure that you've prepared your source data correctly.

These browsers support the Data Import Wizard:

- Google Chrome™ version 29 and later
- Mozilla® Firefox® version 23 and later
- Microsoft® Internet Explorer® version 9 and later
- Apple® Safari® version 5 and later

Note:

- Dragging and dropping CSV files isn't supported in Internet Explorer 9.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

- You can't run more than one import job at a time, even from separate browser windows.

SEE ALSO:

Import Data with the Data Import Wizard

Personalize Your Salesforce Experience

Import Data with the Data Import Wizard

After preparing your data for import, use the Data Import Wizard to map the data fields and run the import.

1. Prepare your data for import and create an import file. Doing this step first prevents errors, duplication of data, and frustration.

   For more information, see the FAQ item "How do I prepare my data for import?" on the Data Import wizard welcome page.

   You can also view the following video playlist to get more information: ▶ Data Import How To Series

2. Start the wizard.

   a. From Setup, enter `Data Import Wizard` in the Quick Find box, then select **Data Import Wizard**.

   b. Review the information provided on the welcome page, then click **Launch Wizard**.

   You can also launch the Data Import Wizard from the Tools list on the object-specific home page.

   Note: Users who aren't administrators can also access the Data Import wizard from their personal settings.

3. Choose the data that you want to import.

   a. To import accounts, contacts, leads, solutions, person accounts, or articles, click **Standard Objects**. To import custom objects, click **Custom Objects**.

   b. Specify whether you want to add new records to Salesforce, update existing records, or add and update records simultaneously.

      Note: If you have workflows that add new objects when importing, selecting **add new and update existing records** fires them, but selecting **update existing records** doesn't.

   c. Specify matching and other criteria as necessary. Hover your mouse over the question marks for more information about each option.

   d. Specify whether to trigger workflow rules and processes when the imported records meet the criteria.

   e. Specify the file that contains your data.

      Specify your data file by dragging the CSV file to the upload area of the page. You can also click the CSV category you're using and then navigate to the file.

   f. Choose a character encoding method for your file. Typically, you don't change your character encoding.

   g. Select comma or tab as a value separator.

   h. Click **Next**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To import data with the Data Import Wizard:

- Depends on what you're importing. See What permissions do I need to import records? in the Salesforce Help.

4. Map your data fields to Salesforce data fields.

   The Data Import wizard maps as many of your data fields as possible to standard Salesforce data fields. But if the wizard can't map fields, you must do it manually. Unmapped fields are not imported into Salesforce.

   To see a list of standard Salesforce data fields, from the management settings for the object, go to the fields area.

   a. Scan the list of mapped data fields and locate the unmapped fields.
   b. Click **Map** to the left of each unmapped field.
   c. In the Map Your Field dialog box, search and choose up to 10 Salesforce fields to map to and click **Map**.

      Note: You also have the option of saving data from unmapped fields in a general notes field for accounts and contacts. Choose **Account Note** or **Contact Note** from the Map To dropdown list and click **Map**.

   d. To change mappings that Salesforce performed automatically, click **Change** to the left of the appropriate field. Delete the Salesforce fields you don't want to map, choose the fields you want to map, then click **Map**.
   e. Click **Next**.

5. Review and start your import.

   a. Review your import information on the Review page. If you still have unmapped fields that you want to import, click **Previous** to return to the previous page and specify your mappings.
   b. Click **Start Import**.

6. Check import status.

   The **Recent Import Jobs** chart on the Data Import Wizard home page lists the status and metrics of the data import. Alternately from Setup, enter `Bulk Data Load Jobs` in the Quick Find box, then select **Bulk Data Load Jobs**.

   Note: The Bulk Data Load Jobs page is not available in Professional Edition. Only administrators have access to the Bulk Data Load Jobs page in Salesforce Setup. If you're not an administrator, you can check the status of your upload by monitoring the relevant tabs in Salesforce.

Need help getting started? Check out www.salesforce.com/gettingstarted to access live webinars, videos, setup series and more. For hands-on help with data importing, complete the Importing Data module in Trailhead.

Add Person Accounts with the Data Import Wizard

To add person accounts to your Salesforce org, launch the Data Import Wizard from the accounts home page.

Before you begin, make sure that your import file is in CSV format and contains values for these fields.

- First Name
- Last Name
- Email
- Phone

Tip: To obtain Salesforce IDs or other values from your org, run reports and then export the report data.

These steps describe one recommended method of importing data. You can import data into Salesforce fields that aren't listed here. You can also customize your import by using other options that appear in the Data Import Wizard.

1. From the accounts home page, click **Import Person Accounts**.
   The Data Import Wizard appears.
2. Select **Person Accounts**, then select **Add new and update existing records**.
3. Set `Match Account by` to **Email**.
4. Select the CSV file that contains your import data, and click **Next**.
5. Map column headers from your CSV file to these fields.
   - First Name
   - Last Name
   - Email
   - Phone
6. Click **Next**.
7. Review the import settings, and then click **Start Import**.

When we finish importing your data, we notify you by email. Review the results and resolve any errors that occurred.

EDITIONS

Data Import Wizard available in both Salesforce Classic and Lightning Experience

Data Import Wizard available in **All** Editions except Database.com

Person accounts available in: both Salesforce Classic and Lightning Experience

Person accounts available in **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To create person accounts that you own via the Data Import Wizard:

- Create on accounts

  AND

  Edit on accounts

  AND

  Import Personal Contacts

To create person accounts owned by others via the Data Import Wizard:

- Create on accounts

  AND

  Edit on accounts and contacts

  AND

  Modify All Data

Data Loader

Data Loader is a client application for the bulk import or export of data. Use it to insert, update, delete, or export Salesforce records.

When importing data, Data Loader reads, extracts, and loads data from comma-separated values (CSV) files or from a database connection. When exporting data, it outputs CSV files.

Note: If commas aren't appropriate for your locale, use a tab or other delimiter. Specify your delimiter in Data Loader Settings (**Settings | Settings**).

You can use Data Loader in two different ways:

- User interface—When you use the user interface, you work interactively to specify the configuration parameters, CSV files used for import and export, and the field mappings that map the field names in your import file with the field names in Salesforce.
- Command line (Windows only)—When you use the command line, you specify the configuration, data sources, mappings, and actions in files. This enables you to set up Data Loader for automated processing.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Data Loader offers the following key features:

- An easy-to-use wizard interface for interactive use
- An alternate command-line interface for automated batch operations (Windows only)
- Support for large files with up to 5 million records
- Drag-and-drop field mapping
- Support for all objects, including custom objects
- Can be used to process data in both Salesforce and Database.com
- Detailed success and error log files in CSV format
- A built-in CSV file viewer
- Support for Windows and Mac

To get started, see the following topics:

- When to Use Data Loader
- Considerations for Installing Data Loader

Note: In previous versions, Data Loader has been known as "AppExchange Data Loader" and "Sforce Data Loader."

SEE ALSO:

Encrypt New Data in Fields

Encrypt New Files and Attachments

When to Use Data Loader

Data Loader complements the web-based import wizards that are accessible from the Setup menu in the online application. Refer to the following guidelines to determine which method best suits your business needs:

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Use Data Loader when:

- You need to load 50,000 to 5,000,000 records. Data Loader is supported for loads of up to 5 million records. If you need to load more than 5 million records, we recommend you work with a Salesforce partner or visit the *App Exchange* for a suitable partner product.
- You need to load into an object that is not yet supported by the import wizards.
- You want to schedule regular data loads, such as nightly imports.
- You want to export your data for backup purposes.

Use the import wizards when:

- You are loading less than 50,000 records.
- The object you need to import is supported by import wizards. To see what import wizards are available and thus what objects they support, from Setup, enter `Data Management` in the `Quick Find` box, then select **Data Management**.
- You want to prevent duplicates by uploading records according to account name and site, contact email address, or lead email address.

For more information about the import wizards, see Import Data Into Salesforce on page 394.

Considerations for Installing Data Loader

Before you download and install Data Loader, understand the system requirements, installation considerations, and login considerations. From Setup, enter `Data Loader` in the Quick Find box, then select **Data Loader**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To access the page to download Data Loader:

- Modify All Data

To use Data Loader:

- API Enabled

  AND

  The appropriate user permission for the operation you are doing, for example, Create on accounts to insert new accounts

  AND

  Bulk API Hard Delete (only if you configure Data Loader to use Bulk API to hard-delete records)

System Requirements for Windows

Data Loader is signed for Windows. To use Data Loader for Windows, you need:

- Microsoft® Windows® 7, Windows® 8, or Windows® 10
- 120 MB of free disk space
- 256 MB of available memory
- Java JRE 1.8 (32-bit)

Note: Salesforce no longer bundles Java with the Data Loader for Windows installer. Download and install Java on your Windows computer.

We recommend that you set the `JAVA_HOME` environment variable to the directory where the Java Runtime Environment (JRE) is installed. Doing so ensures that you can run Data Loader in batch mode from the command line.

System Requirements for macOS

To use Data Loader for macOS, you need:

- macOS El Capitan
- 120 MB of free disk space
- 256 MB of available memory
- Java JRE 1.8
- Administrator privileges on the machine

Installation Considerations

Over time, several versions of the Data Loader client application have been available for download. Some earlier versions were called “AppExchange Data Loader” or “Sforce Data Loader.” You can run different versions at the same time on one computer. However, do not install more than one copy of the same version.

The latest version is always available in Salesforce. If you have installed the latest version and want to install it again, first remove the version on your computer.

Tip: If you experience login issues in the command line interface after upgrading to a new version of Data Loader, please try re-encrypting your password to solve the problem. For information on the password encryption utility, see Encrypt from the Command Line on page 441.

Note: The Data Loader command-line interface is supported for Windows only.

To make changes to the source code, download the open-source version of Data Loader from *https://github.com/forcedotcom/dataloader*.

Login Considerations

- If your organization restricts IP addresses, logins from untrusted IPs are blocked until they're activated. Salesforce automatically sends you an activation email that you can use to log in. The email contains a security token that you must add to the end of your password. For example, if your password is *`mypassword`*, and your security token is *`XXXXXXXXXX`*, you must enter *`mypasswordXXXXXXXXXX`* to log in.
- Data Loader version 36.0 and later supports Web Server OAuth Authentication. See OAuth Authentication for more information.
- Data Loader version 36.0 and later supports Salesforce Communities. Communities users always log in with the OAuth option in Data Loader. To enable OAuth for Communities, the user modifies the `config.properties` file as follows.
  - Change the portion in bold in the following line to the login URL of the community. Don't add a forward slash (/) to the end of the line.

    ```
    sfdc.oauth.Production.server=https\://login.salesforce.com
    ```

    For example:

    ```
    sfdc.oauth.Production.server=
    https\://johnsmith-developer-edition.yourInstance.force.com/test
    ```

  - Change the portion in bold in the following line to the hostname of the community.

    ```
    sfdc.oauth.Production.redirecturi=https\://login.salesforce.com/services/oauth2/success
    ```

    For example:

    ```
    sfdc.oauth.Production.redirecturi=
    https\:/johnsmith-developer-edition.yourInstance.force.com/services/oauth2/success
    ```

  The `config.properties` file is in the `conf` default configuration directory, which is installed in these locations.

  - macOS: `/Applications/Data\ Loader.app/Contents/Resources/conf/`
  - Windows: `%LOCALAPPDATA%\salesforce.com\Data Loader\samples\conf\` for the current user, and `C:\ProgramData\salesforce.com\Data Loader\samples\conf\` for all users

Configure Data Loader

Use the Settings menu to change the Data Loader default operation settings.

1. Open the Data Loader.
2. Select **Settings** > **Settings**.
3. Edit the fields as needed.

Field	Description
`Batch size`	In a single insert, update, upsert, or delete operation, records moving to or from Salesforce are processed in increments of this size. The maximum is 200 records. We recommend a value between 50 and 100. The maximum value is 10,000 if the `Use Bulk API` option is selected.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Field	Description
Insert null values	Select this option to insert blank mapped values as null values during data operations. When you are updating records, this option instructs Data Loader to overwrite existing data in mapped fields. This option is not available if the Use Bulk API option is selected. Empty field values are ignored when you update records using the Bulk API. To set a field value to null when the Use Bulk API option is selected, use a field value of #N/A.
Assignment rule	Specify the ID of the assignment rule to use for inserts, updates, and upserts. This option applies to inserts, updates, and upserts on cases and leads. It also applies to updates on accounts if your organization has territory assignment rules on accounts. The assignment rule overrides Owner values in your CSV file.
Server host	Enter the URL of the Salesforce server with which you want to communicate. For example, if you are loading data into a sandbox, change the URL to https://test.salesforce.com.
Reset URL on Login	By default, Salesforce resets the URL after login to the one specified in Server host. To turn off this automatic reset, disable this option.
Compression	Compression enhances the performance of Data Loader and is turned on by default. You might want to disable compression when debugging the underlying SOAP messages. To turn off compression, enable this option.
Timeout	Specify how many seconds Data Loader waits to receive a response back from the server before returning an error for the request.
Query request size	In a single export or query operation, records are returned from Salesforce in increments of this size. The maximum value is 2,000 records. Larger values may improve performance but use more memory on the client.
Generate status files for exports	Select this option to generate success and error files when exporting data.
Read all CSVs with UTF-8 encoding	Select this option to force files to open in UTF-8 encoding, even if they were saved in a different format.
Write all CSVs with UTF-8 encoding	Select this option to force files to be written in UTF-8 encoding.
Use European date format	Select this option to support the date formats dd/MM/yyyy and dd/MM/yyyy HH:mm:ss.

Field	Description
`Allow field truncation`	Select this option to truncate data in the following types of fields when loading that data into Salesforce: Email, Multi-select Picklist, Phone, Picklist, Text, and Text (Encrypted). In Data Loader versions 14.0 and earlier, values for fields of those types are truncated by Data Loader if they are too large. In Data Loader version 15.0 and later, the load operation fails if a value is specified that is too large. Selecting this option allows you to specify that the previous behavior, truncation, be used instead of the new behavior in Data Loader versions 15.0 and later. This option is selected by default and has no effect in versions 14.0 and earlier. This option is not available if the `Use Bulk API` option is selected. In that case, the load operation fails for the row if a value is specified that is too large for the field.
`Allow comma as a CSV delimiter`	Select this option if your CSV file uses commas to delimit records.
`Allow tab as a CSV delimiter`	Select this option if your CSV file uses tab characters to delimit records.
`Allow other characters as CSV delimiters`	Select this option if your CSV file uses a character other than a comma or tab to delimit records.
`Other delimiters (enter multiple values with no separator; for example, !+?)`	The characters in this field are used only if the **Allow other characters as CSV delimiters** option is selected. For example, if you use the | (pipe) character to delimit data records, enter that character in this field.
`Use Bulk API`	Select this option to use Bulk API to insert, update, upsert, delete, and hard-delete records. Bulk API is optimized to load or delete many records asynchronously. It's faster than the default SOAP-based API due to parallel processing and fewer network round-trips. Warning: You can hard delete records when you configure Data Loader to `Use Bulk API`. Keep in mind that hard deleted records are immediately deleted and can't be recovered from the Recycle Bin.
`Enable serial mode for Bulk API`	To use serial processing instead of parallel processing for Bulk API, select this option. Processing in parallel can cause database contention. When contention is severe, the load can fail. Serial mode processes batches one at a time, however it can increase the processing time for a load. This option is only available if the `Use Bulk API` option is selected.

Field	Description
`Upload Bulk API Batch as Zip File`	Select this option to use Bulk API to upload zip files containing binary attachments, such as Attachment records or Salesforce CRM Content. This option is only available if the `Use Bulk API` option is selected.
`Time Zone`	Select this option to specify a default time zone. If a date value does not include a time zone, this value is used. • If no value is specified, the time zone of the computer where Data Loader is installed is used. • If an incorrect value is entered, GMT is used as the time zone and this fact is noted in the Data Loader log. Valid values are any time zone identifier which can be passed to the Java `getTimeZone(java.lang.String)` method. The value can be a full name such as `America/Los_Angeles`, or a custom ID such as `GMT-8:00`.
`Proxy host`	The host name of the proxy server, if applicable.
`Proxy port`	The proxy server port.
`Proxy username`	The username for proxy server authentication.
`Proxy password`	The password for proxy server authentication.
`Proxy NTLM domain`	The name of the Windows domain used for NTLM authentication.
`Start at row`	If your last operation failed, you can use this setting to begin where the last successful operation finished.

4. Click **OK** to save your settings.

SEE ALSO:

Data Loader Behavior with Bulk API Enabled

Configure the Data Loader to Use the Bulk API

Data Loader Behavior with Bulk API Enabled

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Enabling the Bulk API in Data Loader allows you to load or delete a large number of records faster than using the default SOAP-based API. However, there are some differences in behavior in Data Loader when you enable the Bulk API. One important difference is that it allows you to execute a hard delete if you have the permission and license. See Configure Data Loader on page 427.

The following settings are not available on the **Settings** > **Settings** page in Data Loader when the `Use Bulk API` option is selected:

`Insert null values`

This option enables Data Loader to insert blank mapped values as `null` values during data operations when the Bulk API is disabled. Empty field values are ignored when you update records using the Bulk API. To set a field value to `null` when the `Use Bulk API` option is selected, use a field value of `#N/A`.

`Allow field truncation`

This option directs Data Loader to truncate data for certain field types when the Bulk API is disabled. A load operation fails for the row if a value is specified that is too large for the field when the `Use Bulk API` option is selected.

SEE ALSO:

Configure Data Loader

Configure the Data Loader to Use the Bulk API

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

The Bulk API is optimized to load or delete a large number of records asynchronously. It is faster than the SOAP-based API due to parallel processing and fewer network round-trips. By default, Data Loader uses the SOAP-based API to process records.

To configure Data Loader to use the Bulk API for inserting, updating, upserting, deleting, and hard deleting records:

1. Open the Data Loader.
2. Choose **Settings** > **Settings**.
3. Select the `Use Bulk API` option.
4. Click **OK**.

Note:

- You can also select the `Enable serial mode for Bulk API` option. Processing in parallel can cause database contention. When contention is severe, the load can fail. Serial mode processes batches one at a time, however it can increase the processing time for a load.
- **Caution:** You can hard delete records when you configure Data Loader to `Use Bulk API`. Keep in mind that hard deleted records are immediately deleted and can't be recovered from the Recycle Bin.

SEE ALSO:

Configure Data Loader

Data Types Supported by Data Loader

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Data Loader supports the following data types:

Base64

String path to file (converts the file to a base64–encoded array). Base64 fields are only used to insert or update attachments and Salesforce CRM Content. For more information, see Uploading Attachments on page 437 and Upload Content with the Data Loader on page 438.

Boolean

- True values (case insensitive) = yes, y, true, on, 1
- False values (case insensitive) = no, n, false, off, 0

Date Formats

We recommend you specify dates in the format *yyyy-MM-ddTHH:mm:ss.SSS+/-HHmm*:

- yyyy is the four-digit year
- MM is the two-digit month (01-12)
- dd is the two-digit day (01-31)
- HH is the two-digit hour (00-23)
- mm is the two-digit minute (00-59)
- ss is the two-digit seconds (00-59)
- SSS is the three-digit milliseconds (000-999)
- +/-HHmm is the Zulu (UTC) time zone offset

The following date formats are also supported:

- yyyy-MM-dd'T'HH:mm:ss.SSS'Z'
- yyyy-MM-dd'T'HH:mm:ss.SSS Pacific Standard Time
- yyyy-MM-dd'T'HH:mm:ss.SSSPacific Standard Time
- yyyy-MM-dd'T'HH:mm:ss.SSS PST
- yyyy-MM-dd'T'HH:mm:ss.SSSPST
- yyyy-MM-dd'T'HH:mm:ss.SSS GMT-08:00
- yyyy-MM-dd'T'HH:mm:ss.SSSGMT-08:00
- yyyy-MM-dd'T'HH:mm:ss.SSS -800
- yyyy-MM-dd'T'HH:mm:ss.SSS-800
- yyyy-MM-dd'T'HH:mm:ss
- yyyy-MM-dd HH:mm:ss
- yyyyMMdd'T'HH:mm:ss
- yyyy-MM-dd
- MM/dd/yyyy HH:mm:ss
- MM/dd/yyyy
- yyyyMMdd

Note the following tips for date formats:

- To enable date formats that begin with the day rather than the month, select the Use European date format box in the Settings dialog. European date formats are dd/MM/yyyy and dd/MM/yyyy HH:mm:ss.

- If your computer's locale is east of Greenwich Mean Time (GMT), we recommend that you change your computer setting to GMT in order to avoid date adjustments when inserting or updating records.
- Only dates within a certain range are valid. The earliest valid date is 1700-01-01T00:00:00Z GMT, or just after midnight on January 1, 1700. The latest valid date is 4000-12-31T00:00:00Z GMT, or just after midnight on December 31, 4000. These values are offset by your time zone. For example, in the Pacific time zone, the earliest valid date is 1699-12-31T16:00:00, or 4:00 PM on December 31, 1699.

Double

Standard double string

ID

A Salesforce ID is a case-sensitive 15-character or case–insensitive 18-character alphanumeric string that uniquely identifies a particular record.

Tip: To ensure data quality, make sure that all Salesforce IDs you enter in Data Loader are in the correct case.

Integer

Standard integer string

String

All valid XML strings; invalid XML characters are removed.

Export Data

You can use the Data Loader export wizard to extract data from any Salesforce object. When you export, you can choose to include (**Export All**) or exclude (**Export**) soft-deleted records.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To export records:
- Read on the records

To export all records:
- Read on the records

1. Open the Data Loader.
2. Click **Export** or **Export All**. These commands can also be found in the File menu.
3. Enter your Salesforce username and password. Click **Log in** to log in. After your login completes successfully, click **Next**. (Until you log out or close the program, you will not be asked to log in again.)

   If your organization restricts IP addresses, logins from untrusted IPs are blocked until they're activated. Salesforce automatically sends you an activation email that you can use to log in. The email contains a security token that you must add to the end of your password. For example, if your password is *`mypassword`*, and your security token is *`XXXXXXXXXX`*, you must enter *`mypasswordXXXXXXXXXX`* to log in.

4. Choose an object. For example, select the Account object. If your object name does not display in the default list, check `Show all objects` to see a complete list of objects that you can access. The objects will be listed by localized label name, with developer name noted in parentheses. For object descriptions, see the *SOAP API Developer's Guide*.
5. Click **Browse...** to select the CSV file to which the data will be exported. You can enter a new file name to create a new file or choose an existing file.

   If you select an existing file, the contents of that file are replaced. Click **Yes** to confirm this action, or click **No** to choose another file.

6. Click **Next**.
7. Create a SOQL query for the data export. For example, check `Id` and `Name` in the query fields and click **Finish**. As you follow the next steps, you will see that the CSV viewer displays all the Account names and their IDs. SOQL is the Salesforce Object Query Language that allows you to construct simple but powerful query strings. Similar to the SELECT command in SQL, SOQL allows you to specify the source object, a list of fields to retrieve, and conditions for selecting rows in the source object.

   a. Choose the fields you want to export.

   b. Optionally, select conditions to filter your data set. If you do not select any conditions, all the data to which you have read access will be returned.

   c. Review the generated query and edit if necessary.

   Tip: You can use a SOQL relationship query to include fields from a related object. For example:

```
Select Name, Pricebook2Id, Pricebook2.Name, Product2Id, Product2.ProductCode FROM
PricebookEntry WHERE IsActive = true
```

   Or:

```
Select Id, LastName, Account.Name FROM Contact
```

   When using relationship queries in Data Loader, the fully specified field names are case-sensitive. For example, using `ACCOUNT.NAME` instead of `Account.Name` does not work.

   Data Loader doesn't support nested queries or querying child objects. For example, queries similar to the following return an error:

```
SELECT Amount, Id, Name, (SELECT Quantity, ListPrice,
PriceBookEntry.UnitPrice, PricebookEntry.Name,
PricebookEntry.product2.Family FROM OpportunityLineItems)
FROM Opportunity
```

   Also, Data Loader doesn't support queries that make use of polymorphic relationships. For example, the following query results in an error:

```
SELECT Id, Owner.Name, Owner.Type, Owner.Id, Subject FROM Case
```

   For more information on SOQL, see the *Force.com SOQL and SOSL Reference*.

8. Click **Finish**, then click **Yes** to confirm.
9. A progress information window reports the status of the operation.
10. After the operation completes, a confirmation window summarizes your results. Click **View Extraction** to view the CSV file, or click **OK** to close. For more details, see Review Data Loader Output Files on page 439.

Note:

- Data Loader currently does not support the extraction of attachments. As a workaround, we recommend that you use the weekly export feature in the online application to export attachments.
- If you select compound fields for export in the Data Loader, they cause error messages. To export values, use individual field components.

Define Data Loader Field Mappings

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

When you insert, delete, or update files, use the Mapping Dialog window to associate Salesforce fields with the columns of your CSV file. For more information, see Insert, Update, or Delete Data Using Data Loader on page 435.

1. To automatically match fields with columns, click **Auto-Match Fields to Columns**. The Data Loader populates the list at the bottom of the window based on the similarity of field and column names. For a delete operation, automatic matching works only on the ID field.
2. To manually match fields with columns, click and drag fields from the list of Salesforce fields at the top to the list of CSV column header names at the bottom. For example, if you are inserting new Account records where your CSV file contains the names of new accounts, click and drag the `Name` field to the right of the `NAME` column header field.
3. Optionally, click **Save Mapping** to save this mapping for future use. Specify a name for the SDL mapping file.

   If you select an existing file, the contents of that file are replaced. Click **Yes** to confirm this action, or click **No** to choose another file.

4. Click **OK** to use your mapping for the current operation.

Insert, Update, or Delete Data Using Data Loader

USER PERMISSIONS

To insert records:	Create on the record
To update records:	Edit on the record
To upsert records:	Create or Edit on the record
To delete records:	Delete on the record
To hard delete records:	Delete on the record
To mass delete records:	Modify All Data

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Use the Data Loader wizards to add, modify, or delete records. The upsert wizard combines inserting and updating a record. If a record in your file matches an existing record, the existing record is updated with the values in your file. If no match is found, a new record is created. When you hard-delete records, the deleted records are not stored in the Recycle Bin and are eligible for deletion. For more information, see Configure Data Loader.

1. Open the Data Loader.
2. Click **Insert**, **Update**, **Upsert**, **Delete**, or **Hard Delete**. These commands are also listed in the File menu.
3. Enter your Salesforce username and password. To log in, click **Log in**. When you are logged in, click **Next**. (Until you log out or close the program, you are not asked to log in again.)

   If your organization restricts IP addresses, logins from untrusted IPs are blocked until they're activated. Salesforce automatically sends you an activation email that you can use to log in. The email contains a security token that you must add to the end of your password. For example, if your password is *`mypassword`*, and your security token is *`XXXXXXXXXX`*, you must enter *`mypasswordXXXXXXXXXX`* to log in.

4. Choose an object. For example, if you are inserting Account records, select **Account**. If your object name does not display in the default list, select **Show all objects** to see a complete list of the objects that you can access. The objects are listed by localized label name, with the developer name noted in parentheses. For object descriptions, see the *Object Reference for Salesforce and Force.com*.

   Note: Data Loader deletes records based on the IDs in the CSV file, not the object selected.

5. To select your CSV file, click **Browse**. For example, if you are inserting Account records, you could specify a CSV file called `insertaccounts.csv` containing a Name column for the names of the new accounts.
6. Click **Next**. After the object and CSV file are initialized, click **OK**.
7. If you are performing an upsert, your CSV file must contain a column of ID values for matching against existing records. The column is either an external ID (a custom field with the External ID attribute) or ID (the Salesforce record ID).
   a. From the dropdown list, select which field to use for matching. If the object has no external ID fields, ID is used. Click **Next** to continue.
   b. If your file includes the external IDs of an object that has a relationship to your chosen object, enable that external ID for record matching by selecting its name from the dropdown list. If you make no selection, you can use the related object's ID field for matching by mapping it in the next step. Click **Next** to continue.
8. Define how the columns in your CSV file map to Salesforce fields. To select an existing field mapping, click **Choose an Existing Map**. To create or modify a map, click **Create or Edit a Map**. For more information, see Define Data Loader Field Mappings on page 435. Click **Next**.
9. For each operation, the Data Loader generates two unique CSV log files. One file name starts with "success," and the other starts with "error." Click **Browse** to specify a directory for these files.
10. To complete the operation, click **Finish**, and then click **Yes** to confirm. As the operation proceeds, a progress information window reports the status of the data movement.
11. To view your success or error files, click **View Successes** or **View Errors**. To close the wizard, click **OK** . For more information, see Review Data Loader Output Files on page 439.

Tip:

- If you are updating or deleting large amounts of data, review Perform Mass Updates and Perform Mass Deletes for tips and best practices.
- There is a 5-minute limit to process 100 records when the Bulk API is enabled. If it takes longer than 10 minutes to process a file, the Bulk API places the remainder of the file back in the queue for later processing. If the Bulk API continues to exceed the 10-minute limit on subsequent attempts, the file is placed back in the queue and reprocessed up to 10 times before the operation is permanently marked as failed. Even if the processing fails, some records could have completed successfully, so check the results. If you get a timeout error when loading a file, split your file into smaller files and try again.

Perform Mass Updates

To update a large number of records at one time, we recommend the following steps:

1. Obtain your data by performing an export of the objects you wish to update, or by running a report. Make sure your report includes the record ID.
2. As a backup measure, save an extra copy of the generated CSV file.
3. Open your working file in a CSV editor such as Excel, and update your data.
4. Launch Data Loader and follow the update wizard. Note that matching is done according to record ID. See Insert, Update, or Delete Data Using Data Loader on page 435.
5. After the operation, review your success and error log files. See Review Data Loader Output Files on page 439.
6. If you made a mistake, use the backup file to update the records to their previous values.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Perform Mass Deletes

To delete a large number of records at one time using Data Loader, we recommend the following steps:

1. As a backup measure, export the records you wish to delete, being sure to select all fields. (See Export Data on page 433.) Save an extra copy of the generated CSV file.
2. Next, export the records you wish to delete, this time using only the record ID as the desired criterion.
3. Launch the Data Loader and follow the delete or hard delete wizard. Map only the ID column. See Insert, Update, or Delete Data Using Data Loader on page 435.
4. After the operation, review your success and error log files. See Review Data Loader Output Files on page 439.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To mass delete records:
- Modify All Data

Uploading Attachments

You can use Data Loader to upload attachments to Salesforce. Before uploading attachments, note the following:

- If you intend to upload via the Bulk API, verify that `Upload Bulk API Batch as Zip File` on the **Settings** > **Settings** page is enabled.
- If you are migrating attachments from a source Salesforce organization to a target Salesforce organization, begin by requesting a data export for the source organization. On the Schedule Export page, make sure to select the `Include Attachments...` checkbox, which causes the file `Attachment.csv` to be included in your export. You can use this CSV file to upload the attachments. For more information on the export service, see Export Backup Data from Salesforce on page 479.

To upload attachments:

1. Confirm that the CSV file you intend to use for attachment importing contains the following required columns (each column represents a Salesforce field):
   - `ParentId` - the Salesforce ID of the parent record.
   - `Name` - the name of the attachment file, such as `myattachment.jpg`.
   - `Body` - the absolute path to the attachment on your local drive.

Ensure that the values in the `Body` column contain the full file name of the attachments as they exist on your computer. For example, if an attachment named `myattachment.jpg` is located on your computer at `C:\Export`, `Body` must specify `C:\Export\myattachment.jpg`. Your CSV file might look like this:

```
ParentId,Name,Body
50030000000VDowAAG,attachment1.jpg,C:\Export\attachment1.gif
701300000000iNHAAY,attachment2.doc,C:\Export\files\attachment2.doc
```

The CSV file can also include other optional Attachment fields, such as `Description`.

2. Proceed with an insert or upsert operation; see Insert, Update, or Delete Data Using Data Loader on page 435. At the `Select data objects` step, make sure to select the `Show all Salesforce objects` checkbox and the `Attachment` object name in the list.

Upload Content with the Data Loader

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

You can use Data Loader to bulk upload documents and links into libraries in Salesforce CRM Content. Before uploading documents or links, note the following.

- If you intend to upload via the Bulk API, verify that `Upload Bulk API Batch as Zip File` on the **Settings** > **Settings** page is enabled.
- When you upload a document from your local drive using Data Loader, specify the path in the `VersionData` and `PathOnClient` fields in the CSV file. `VersionData` identifies the location and extracts the format, and `PathOnClient` identifies the type of document being uploaded.
- When you upload a link using the Data Loader, specify the URL in `ContentUrl`. Don't use `PathOnClient` or `VersionData` to upload links.
- You can't export content using the Data Loader.
- If you're updating content that you've already uploaded:
  - Perform the Insert function.
  - Include a `ContentDocumentId` column with an 18-character ID. Salesforce uses this information to determine that you're updating content. When you map the `ContentDocumentId`, the updates are added to the content file. If you don't include the ContentDocumentId, the content is treated as new, and the content file isn't updated.

1. Create a CSV file with the following fields.
   - `Title` - file name.
   - `Description` - (optional) file or link description.

     Note: If there are commas in the description, use double quotes around the text.

   - `VersionData` - complete file path on your local drive (for uploading documents only).

     Note: Files are converted to base64 encoding on upload. This action adds approximately 30% to the file size.

   - `PathOnClient` - complete file path on your local drive (for uploading documents only).
   - `ContentUrl` - URL (for uploading links only).
   - `OwnerId` - (optional) file owner, defaults to the user uploading the file.
   - `FirstPublishLocationId` - library ID.
   - `RecordTypeId` - record type ID.

> Note: If you publish to a library that has restricted record types, specify `RecordTypeId`.

To determine the `RecordTypeId` values for your organization using Data Loader, follow the steps in Exporting Data. The following is a sample SOQL query:

```
Select Id, Name FROM RecordType WHERE SobjectType = 'ContentVersion'
```

To determine the `RecordTypeId` values for your organization using the AJAX Toolkit:

a. Log in to Salesforce.

b. Enter this URL in your browser: `http://`***`instanceName`***`.salesforce.com/soap/ajax/41.0/debugshell.html`. Enter the *`instanceName`* for your organization. You can see the *`instanceName`* in the URL field of your browser after logging in to Salesforce.

c. In the AJAX Toolkit Shell page, type:

```
sforce.connection.describeSObject("ContentVersion")
```

d. Press **Enter**.

e. Click the arrows for `recordTypeInfos`.

The `RecordTypeId` values for your organization are listed.

- `TagsCsv` - (optional) tag.

A sample CSV file is:

```
Title,Description,VersionData,PathOnClient,OwnerId,FirstPublishLocationId,RecordTypeId,TagsCsv
testfile,"This is a test file, use for bulk
upload",c:\files\testfile.pdf,c:\files\testfile.pdf,005000000000000,058700000004Cd0,012300000008o2sAQG,one
```

2. Upload the CSV file for the ContentVersion object (see Insert, Update, or Delete Data Using Data Loader on page 435). All documents and links are available in the specified library.

Review Data Loader Output Files

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

After an import or export, Data Loader generates two CSV output files that contain the results of the operation. One file name starts with "success," and the other starts with "error." You can use the Data Loader CSV file viewer to open the files.

1. Choose **View** > **View CSV**.
2. Specify the number of rows to view. Each row in the CSV file corresponds to one Salesforce record. The default is 1,000.
3. To view a specific CSV file, click **Open CSV**. To view the last success file, click **Open Success**. To view the last error file, click **Open Error**.
4. To open the file in an external program, such as Excel, click **Open in External Program**.

   The success file contains all the successfully loaded records. The file includes a column with the newly generated record IDs. The error file contains all the rejected records. The file has a column that describes why the load failed.

   > Note: If the object you are exporting has a column named "success" or "error," your output file columns could display incorrect information. To avoid this problem, rename the columns.

5. To return to the CSV Chooser window, click **Close**. To exit the window, click **OK**.

> Note: To generate success files when exporting data, select `Generate status files for exports`. For more information, see Configure Data Loader on page 427.

View the Data Loader Log File

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

If you need to investigate a problem with Data Loader, or if requested by Salesforce Customer Support, you can access log files that track the operations and network connections made by Data Loader.

The log file, `sdl.log`, contains a detailed chronological list of Data Loader log entries. Log entries marked "INFO" are procedural items, such as logging in to and out of Salesforce. Log entries marked "ERROR" are problems such as a submitted record missing a required field. The log file can be opened with commonly available text editor programs, such as Microsoft Notepad.

If you are using Data Loader for Windows, view the log file by entering *`%TEMP%\sdl.log`* in either the Run dialog or the Windows Explorer address bar.

If you are using Data Loader for Mac OSX, view the log file by opening terminal and entering *`open $TMPDIR/sdl.log`*.

If you are having login issues from the command line, ensure that the password provided in the configuration parameters is encrypted. If you are having login issues from the UI, you may need to obtain a new security token.

Batch Mode

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

> Note: The Data Loader command-line interface is supported for Windows only.

You can run Data Loader in batch mode from the command line. See the following topics:

- Installed Directories and Files
- Encrypt from the Command Line
- Upgrade Your Batch Mode Interface
- Data Loader Command-Line Interface
- Configure Batch Processes
- Data Loader Process Configuration Parameters
- Data Loader Command-Line Operations
- Configure Database Access
- Map Columns
- Run Individual Batch Processes
- Data Access Objects

> Note: If you have used the batch mode from the command line with a version earlier than 8.0, see Upgrade Your Batch Mode Interface on page 442.

Installed Directories and Files

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Note: The Data Loader command-line interface is supported for Windows only.

In versions 8.0 and later, installing the Data Loader creates several directories under the installation directory. The following directories are involved in running the program from the command line for automated batch processing:

bin

Contains the batch files `encrypt.bat` for encrypting passwords and `process.bat` for running batch processes.

For information on running the Data Loader from the command line, see Data Loader Command-Line Interface on page 442.

conf

The default configuration directory. Contains the configuration files `config.properties`, `Loader.class`, and `log-conf.xml`.

The `config.properties` file that is generated when you modify the Settings dialog in the graphical user interface is located at `C:\Documents and Settings\`*`your Windows username`*`\Application Data\Salesforce\Data Loader `*`version_number`*. You can copy this file to the `conf` installation directory to use it for batch processes.

The `log-conf.xml` file is included with version 35.0 of the Data Loader for Windows installer. The `log-conf.xml` is located at `%LOCALAPPDATA%\salesforce.com\Data Loader\samples\conf\log-conf.xml` for the current user, and `C:\Program Files (x86)\salesforce.com\Data Loader\samples\conf\log-conf.xml` for all users.

samples

Contains subdirectories of sample files for reference.

File Path Convention

The file paths provided in these topics start one level below the installation directory. For example, `\bin` means `C:\Program Files \Salesforce\Data Loader `*`version_number`*`\bin`, provided you accepted the default installation directory. If you installed the program to a different location, please substitute that directory path as appropriate.

Encrypt from the Command Line

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Note: The Data Loader command-line interface is supported for Windows only.

When running Data Loader in batch mode from the command line, you must encrypt the following configuration parameters:

- `sfdc.password`
- `sfdc.proxyPassword`

Data Loader offers an encryption utility to secure passwords specified in configuration files. This utility is used to encrypt passwords, but data that you transmit using Data Loader is not encrypted.

1. Run `\bin\encrypt.bat`.
2. At the command line, follow the prompts provided to execute the following actions:

   Generate a key

   Key text is generated on screen from the text you provide. Carefully copy the key text to a key file, omitting any leading or trailing spaces. The key file can then be used for encryption and decryption.

Encrypt text

Generates an encrypted version of a password or other text. Optionally, you can provide a key file for the encryption. In the configuration file, make sure that the encrypted text is copied precisely and the key file is mentioned.

Verify encrypted text

Given encrypted and decrypted versions of a password, verifies whether the encrypted password provided matches its decrypted version. A success or failure message is printed to the command line.

Upgrade Your Batch Mode Interface

Note: The Data Loader command-line interface is supported for Windows only.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

The batch mode interface in Data Loader versions 8.0 and later aren't backward-compatible with earlier versions. If you're using a version earlier than 8.0 to run batch processes, your options are as follows:

Maintain the old version for batch use

Do not uninstall your old version of Data Loader. Continue to use that version for batch processes. You can't take advantage of newer features such as database connectivity, but your integrations will continue to work. Optionally, install the new version alongside the old version and dedicate the old version solely to batch processes.

Generate a new config.properties file from the new GUI

If you originally generated your `config.properties` file from the graphical user interface, use the new version to set the same properties and generate a new file. Use this new file with the new batch mode interface. For more information, see Data Loader Command-Line Interface on page 442.

Manually update your config.properties file

If your old `config.properties` file was created manually, you must manually update it for the new version. For more information, see Installed Directories and Files on page 441.

Data Loader Command-Line Interface

Note: The Data Loader command-line interface is supported for Windows only.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

For automated batch operations such as nightly scheduled loads and extractions, run Data Loader from the command line. Before running any batch operation, be sure to include your encrypted password in the configuration file. For more information, see Data Loader Command Line Introduction on page 459 and Encrypt from the Command Line on page 441. From the command line, navigate to the `bin` directory and type *`process.bat`*, which takes the following parameters:

- The directory containing `config.properties`.
- The name of the batch process bean contained in `process-conf.xml`.

The `log-conf.xml` file is included with version 35.0 of the Data Loader for Windows installer. The `log-conf.xml` is located at `%LOCALAPPDATA%\salesforce.com\Data Loader\samples\conf\log-conf.xml` for the current user, and `C:\Program Files (x86)\salesforce.com\Data Loader\samples\conf\log-conf.xml` for all users.

For more information about using *`process.bat`*, see Run Individual Batch Processes on page 458.

To view tips and instructions, add *`-help`* to the command contained in *`process.bat`*.

Data Loader runs whatever operation, file, or map is specified in the configuration file that you specify. If you do not specify a configuration directory, the current directory is used. By default, Data Loader configuration files are installed at the following location:

```
C:\Program Files\Salesforce\Data Loader version number\conf
```

You use the `process-conf.xml` file to configure batch processing. Set the name of the process in the bean element's id attribute: (for example <bean id="myProcessName">).

If you want to implement enhanced logging, use a copy of `log-conf.xml`.

You can change parameters at runtime by giving *`param=value`* as program arguments. For example, adding `process.operation=insert` to the command changes the configuration at runtime.

You can set the minimum and maximum heap size. For example, `-Xms256m -Xmx256m` sets the heap size to 256 MB.

Note: These topics only apply to Data Loader version 8.0 and later.

Tip: If you experience login issues in the command line interface after upgrading to a new version of Data Loader, please try re-encrypting your password to solve the problem. For information on the password encryption utility, see Encrypt from the Command Line on page 441.

Configure Batch Processes

Note: The Data Loader command-line interface is supported for Windows only.

Use `\samples\conf\process-conf.xml` to configure your Data Loader processes, which are represented by ProcessRunner beans. A process should have `ProcessRunner` as the `class` attribute and the following properties set in the configuration file:

name

Sets the name of the ProcessRunner bean. This value is also used as the non-generic thread name and for configuration backing files (see below).

configOverrideMap

A property of type `map` where each entry represents a configuration setting: the key is the setting name; the value is the setting value.

enableLastRunOutput

If set to true (the default), output files containing information about the last run, such as `sendAccountsFile_lastrun.properties`, are generated and saved to the location specified by `lastRunOutputDirectory`. If set to false, the files are not generated or saved.

lastRunOutputDirectory

The directory location where output files containing information about the last run, such as `sendAccountsFile_lastrun.properties`, are written. The default value is `\conf`. If `enableLastRunOutput` is set to false, this value is not used because the files are not generated.

The configuration backing file stores configuration parameter values from the last run for debugging purposes, and is used to load default configuration parameters in `config.properties`. The settings in `configOverrideMap` take precedence over those in the configuration backing file. The configuration backing file is managed programmatically and does not require any manual edits.

For the names and descriptions of available process configuration parameters, see Data Loader Process Configuration Parameters on page 444.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Data Loader Process Configuration Parameters

Note: The Data Loader command-line interface is supported for Windows only.

When running Data Loader from the command line, you can specify the following configuration parameters in the `process-conf.xml` file. In some cases, the parameter is also represented in the UI at **Settings** > **Settings**.

Tip: A sample `process-conf.xml` file is in the `\samples` directory that's installed with Data Loader.

Parameter Name	Data Type	Equivalent Option in Settings Dialog	Description
`dataAccess.readUTF8`	boolean	`Read all CSVs with UTF-8 encoding`	Select this option to force files to open in UTF-8 encoding, even if they were saved in a different format. Sample value: `true`
`dataAccess.writeUTF8`	boolean	`Write all CSVs with UTF-8 encoding`	Select this option to force files to be written in UTF-8 encoding. Sample value: `true`
`dataAccess.name`	string	Not applicable (N/A)	Name of the data source to use, such as a CSV file name. For databases, use the name of the database configuration in `database-conf.xml`. Sample value: `c:\dataloader\data\extractLead.csv`
`dataAccess.readBatchSize`	integer	N/A	Number of records read from the database at a time. The maximum value is 200. Sample value: `50`
`dataAccess.type`	string	N/A	Standard or custom data source type. Standard types are `csvWriter`, `csvRead`, `databaseWrite`, and `databaseRead`. Sample value: `csvWrite`

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Parameter Name	Data Type	Equivalent Option in Settings Dialog	Description
`dataAccess.writeBatchSize`	integer	N/A	Number of records written to the database at a time. The maximum value is 2,000. Note the implication for a large parameter value: if an error occurs, all records in the batch are rolled back. In contrast, if the value is set to 1, each record is processed individually (not in batch) and errors are specific to a given record. We recommend setting the value to 1 when you need to diagnose problems with writing to a database. Sample value: `500`
`loader.csvComma`	boolean	`Allow comma as a CSV delimiter`	Select this option if your CSV file uses commas to delimit records.
`loader.csvTab`	boolean	`Allow tab as a CSV delimiter`	Select this option if your CSV file uses tab characters to delimit records.
`loader.csvOther`	boolean	`Allow other characters as CSV delimiters`	Select this option if your CSV file uses a character other than a comma or tab to delimit records.
`loader.csvOtherValue`	string	`Other delimiters (enter multiple values with no separator; for example, !+?)`	The characters in this field are used only if the **Allow other characters as CSV delimiters** option is selected. For example, if you use the | (pipe) character to delimit data records, enter that character in this field.
`process.enableExtractStatusOutput`	boolean	`Generate status files for exports`	Select this option to generate success and error files when exporting data. Sample value: `true`
`process.enableLastRunOutput`	boolean	N/A	When running Data Loader in batch mode, you can disable the generation of output files such as

Parameter Name	Data Type	Equivalent Option in Settings Dialog	Description
			`sendAccountsFile_lastRun.properties`. Files of this type are saved by default to the `conf` directory. To stop the writing of these files, set this option to `false`. Alternatively, you can change the location of the directory where these files are saved, using `process.lastRunOutputDirectory`. Sample value: `true`
`process.encryptionKeyFile`	string (file name)	N/A	Name of the file that contains the encryption key. See Encrypt from the Command Line on page 441. Sample value: `c:\dataloader\conf\my.key`
`process.initialLastRunDate`	date	N/A	The initial setting for the `process.lastRunDate` parameter, which can be used in a SQL string and is automatically updated when a process has run successfully. For an explanation of the date format syntax, see Date Formats on page 432. Format must be `yyyy-MM-ddTHH:mm:ss.SSS+/-HHmm`. For example: 2006-04-13T13:50:32.423-0700
`process.lastRunOutputDirectory`	string (directory)	N/A	When running Data Loader in batch mode, you can change the location where output files such as `sendAccountsFile_lastRun.properties` are written. Files of this type are saved by default to the `\conf` directory. To change the location, change the value of this option to the full path where the output files should be written. Alternatively, you can stop the files from being written, using `process.enableLastRunOutput`.
`process.loadRowToStartAt`	number	`Start at row`	If your last operation failed, you can use this setting to begin where the last successful operation finished. Sample value: `1008`
`process.mappingFile`	string (file name)	N/A	Name of the field mapping file to use. See Map Columns on page 457. Sample value: `c:\dataloader\conf\accountExtractMap.sdl`

Parameter Name	Data Type	Equivalent Option in Settings Dialog	Description
process.operation	string	N/A	The operation to perform. See Data Loader Command-Line Operations on page 452. Sample value: extract
process.statusOutputDirectory	string (directory)	N/A	The directory where "success" and "error" output files are saved. The file names are automatically generated for each operation unless you specify otherwise in process-conf.xml. Sample value: c:\dataloader\status
process.outputError	string (file name)	N/A	The name of the CSV file that stores error data from the last operation. Sample value: c:\dataloader\status\myProcessErrors.csv
process.outputSuccess	string (file name)	N/A	The name of the CSV file that stores success data from the last operation. See also process.enableExtractStatusOutput on page 445. Sample value: c:\dataloader\status\myProcessSuccesses.csv
process.useEuropeanDates	boolean	Use European date format	Select this option to support the date formats dd/MM/yyyy and dd/MM/yyyy HH:mm:ss. Sample value: true
sfdc.assignmentRule	string	Assignment rule	Specify the ID of the assignment rule to use for inserts, updates, and upserts. This option applies to inserts, updates, and upserts on cases and leads. It also applies to updates on accounts if your organization has territory assignment rules on accounts. The assignment rule overrides Owner values in your CSV file. Sample value: 03Mc00000026J7w
sfdc.bulkApiCheckStatusInterval	integer	N/A	The number of milliseconds to wait between successive checks to determine if the asynchronous Bulk API operation is complete or how many records have been processed. See also sfdc.useBulkApi. We recommend a value of 5000. Sample value: 5000

Parameter Name	Data Type	Equivalent Option in Settings Dialog	Description
`sfdc.bulkApiSerialMode`	boolean	`Enable serial mode for Bulk API`	To use serial processing instead of parallel processing for Bulk API, select this option. Processing in parallel can cause database contention. When contention is severe, the load can fail. Serial mode processes batches one at a time, however it can increase the processing time for a load. See also `sfdc.useBulkApi`. Sample value: `false`
`sfdc.bulkApiZipContent`	boolean	`Upload Bulk API Batch as Zip File`	Select this option to use Bulk API to upload zip files containing binary attachments, such as Attachment records or Salesforce CRM Content. See also `sfdc.useBulkApi`. Sample value: `true`
`sfdc.connectionTimeoutSecs`	integer	N/A	The number of seconds to wait for a connection during API calls. Sample value: `60`
`sfdc.debugMessages`	boolean	N/A	If true, enables SOAP message debugging. By default, messages are sent to STDOUT unless you specify an alternate location in `sfdc.debugMessagesFile`. Sample value: `false`
`sfdc.debugMessagesFile`	string (file name)	N/A	See `process.enableExtractStatusOutput` on page 445. Stores SOAP messages sent to or from Salesforce. As messages are sent or received, they are appended to the end of the file. As the file does not have a size limit, please monitor your available disk storage appropriately. Sample value: `\lexiloader\status\sfdcSoapTrace.log`
`sfdc.enableRetries`	boolean	N/A	If true, enables repeated attempts to connect to Salesforce servers. See `sfdc.maxRetries` on page 449 and `sfdc.minRetrySleepSecs` on page 450. Sample value: `true`
`sfdc.endpoint`	URL	`Server host`	Enter the URL of the Salesforce server with which you want to communicate. For example, if you are loading

Parameter Name	Data Type	Equivalent Option in Settings Dialog	Description
			data into a sandbox, change the URL to `https://test.salesforce.com`. Sample production value: `https://login.salesforce.com/services/Soap/u/41.0`
`sfdc.entity`	string	N/A	The Salesforce object used in the operation. Sample value: `Lead`
`sfdc.externalIdField`	string	N/A	Used in upsert operations; specifies the custom field with the “External ID” attribute that is used as a unique identifier for data matching. Sample value: `LegacySKU__c`
`sfdc.extractionRequestSize`	integer	`Query request size`	In a single export or query operation, records are returned from Salesforce in increments of this size. The maximum value is 2,000 records. Larger values may improve performance but use more memory on the client. Sample value: `500`
`sfdc.extractionSOQL`	string	N/A	The SOQL query for the data export. Sample value: `SELECT Id, LastName, FirstName, Rating, AnnualRevenue, OwnerId FROM Lead`
`sfdc.insertNulls`	boolean	`Insert null values`	Select this option to insert blank mapped values as `null` values during data operations. When you are updating records, this option instructs Data Loader to overwrite existing data in mapped fields. Sample value: `false`
`sfdc.loadBatchSize`	integer	`Batch size`	In a single insert, update, upsert, or delete operation, records moving to or from Salesforce are processed in increments of this size. The maximum is 200 records. We recommend a value between 50 and 100. Sample value: `100`
`sfdc.maxRetries`	integer	N/A	The maximum number of repeated attempts to connect to Salesforce. See `sfdc.enableRetries` on page 448. Sample value: `3`

Parameter Name	Data Type	Equivalent Option in Settings Dialog	Description
sfdc.minRetrySleepSecs	integer	N/A	The minimum number of seconds to wait between connection retries. The wait time increases with each try. See sfdc.enableRetries on page 448. Sample value: 2
sfdc.noCompression	boolean	Compression	Compression enhances the performance of Data Loader and is turned on by default. You might want to disable compression when debugging the underlying SOAP messages. To turn off compression, enable this option. Sample value: false
sfdc.password	encrypted string	N/A	An encrypted Salesforce password that corresponds to the username provided in sfdc.username. See also Encrypt from the Command Line on page 441. Sample value: 4285b36161c65a22
sfdc.proxyHost	URL	Proxy host	The host name of the proxy server, if applicable. Sample value: http://myproxy.internal.company.com
sfdc.proxyPassword	encrypted string	Proxy password	An encrypted password that corresponds to the proxy username provided in sfdc.proxyUsername. See also Encrypt from the Command Line on page 441. Sample value: 4285b36161c65a22
sfdc.proxyPort	integer	Proxy port	The proxy server port. Sample value: 8000
sfdc.proxyUsername	string	Proxy username	The username for proxy server authentication. Sample value: jane.doe
sfdc.resetUrlOnLogin	boolean	Reset URL on Login	By default, Salesforce resets the URL after login to the one specified in sfdc.endpoint. To turn off this automatic reset, disable this option by setting it to false. Valid values: true (default), false

Parameter Name	Data Type	Equivalent Option in Settings Dialog	Description
sfdc.timeoutSecs	integer	Timeout	Specify how many seconds Data Loader waits to receive a response back from the server before returning an error for the request. Sample value: 540
sfdc.timezone	string	Time Zone	If a date value does not include a time zone, this value is used. - If no value is specified, the time zone of the computer where Data Loader is installed is used. - If an incorrect value is entered, GMT is used as the time zone and this fact is noted in the Data Loader log. Valid values are any time zone identifier which can be passed to the Java getTimeZone(java.lang.String) method. The value can be a full name such as America/Los_Angeles, or a custom ID such as GMT-8:00. You can retrieve the default value by running the TimeZone.getDefault() method in Java. This value is the time zone on the computer where Data Loader is installed.
sfdc.truncateFields	boolean	Allow field truncation	Select this option to truncate data in the following types of fields when loading that data into Salesforce: Email, Multi-select Picklist, Phone, Picklist, Text, and Text (Encrypted). In Data Loader versions 14.0 and earlier, values for fields of those types are truncated by Data Loader if they are too large. In Data Loader version 15.0 and later, the load operation fails if a value is specified that is too large. Selecting this option allows you to specify that the previous behavior, truncation, be used instead of the new behavior in Data Loader versions 15.0 and later. This option is selected by default and has no effect in versions 14.0 and earlier. This option is not available if the Use Bulk API option is selected. In that case, the load operation fails for the row if a value is specified that is too large for the field.

Parameter Name	Data Type	Equivalent Option in Settings Dialog	Description
			Sample value: `true`
`sfdc.useBulkApi`	boolean	`Use Bulk API`	Select this option to use Bulk API to insert, update, upsert, delete, and hard-delete records. Bulk API is optimized to load or delete many records asynchronously. It's faster than the default SOAP-based API due to parallel processing and fewer network round-trips. See also `sfdc.bulkApiSerialMode`. Sample value: `true`
`sfdc.username`	string	N/A	Salesforce username. See `sfdc.password`. Sample value: `jdoe@mycompany.com`

Data Loader Command-Line Operations

Note: The Data Loader command-line interface is supported for Windows only.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

When running Data Loader in batch mode from the command line, several operations are supported. An operation represents the flow of data between Salesforce and an external data source such as a CSV file or a database. See the following list of operation names and descriptions.

Extract

Uses a Salesforce Object Query Language to export a set of records from Salesforce, then writes the exported data to a data source. Soft-deleted records are not included.

Extract All

Uses a Salesforce Object Query Language to export a set of records from Salesforce, including both existing and soft-deleted records, then writes the exported data to a data source.

Insert

Loads data from a data source into Salesforce as new records.

Update

Loads data from a data source into Salesforce, where existing records with matching ID fields are updated.

Upsert

Loads data from a data source into Salesforce, where existing records with a matching custom external ID field are updated; records without matches are inserted as new records.

Delete

Loads data from a data source into Salesforce, where existing records with matching ID fields are deleted.

Hard Delete

Loads data from a data source into Salesforce, where existing records with matching ID fields are deleted without being stored first in the Recycle Bin.

Configure Database Access

Note: The Data Loader command-line interface is supported for Windows only.

When you run Data Loader in batch mode from the command line, use `\samples\conf\database-conf.xml` to configure database access objects, which you use to extract data directly from a database.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

DatabaseConfig Bean

The top-level database configuration object is the `DatabaseConfig` bean, which has the following properties:

sqlConfig
The SQL configuration bean for the data access object that interacts with a database.

dataSource
The bean that acts as database driver and authenticator. It must refer to an implementation of `javax.sql.DataSource` such as `org.apache.commons.dbcp.BasicDataSource`.

The following code is an example of a DatabaseConfig bean:

```
<bean id="AccountInsert"
    class="com.salesforce.dataloader.dao.database.DatabaseConfig"
    singleton="true">
    <property name="sqlConfig" ref="accountInsertSql"/>
</bean>
```

DataSource

The `DataSource` bean sets the physical information needed for database connections. It contains the following properties:

driverClassName
The fully qualified name of the implementation of a JDBC driver.

url
The string for physically connecting to the database.

username
The username for logging in to the database.

password
The password for logging in to the database.

Depending on your implementation, additional information may be required. For example, use `org.apache.commons.dbcp.BasicDataSource` when database connections are pooled.

The following code is an example of a DataSource bean:

```
<bean id="oracleRepDataSource"
    class="org.apache.commons.dbcp.BasicDataSource"
    destroy-method="close">
    <property name="driverClassName" value="oracle.jdbc.driver.OracleDriver"/>
    <property name="url" value="jdbc:oracle:thin:@myserver.salesforce.com:1521:TEST"/>
    <property name="username" value="test"/>
    <property name="password" value="test"/>
</bean>
```

Versions of Data Loader from API version 25.0 onwards do not come with an Oracle JDBC driver. Using Data Loader to connect to an Oracle data source without a JDBC driver installed will result in a "Cannot load JDBC driver class" error. To add the Oracle JDBC driver to Data Loader:

- Download the latest JDBC driver from `http://www.oracle.com/technetwork/database/features/jdbc/index-091264.html`.
- Copy the JDBC .jar file to *`data loader install folder`*`/java/bin`.

SEE ALSO:

Spring Framework

Data Access Objects

SQL Configuration

Spring Framework

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Note: The Data Loader command-line interface is supported for Windows only.

The Data Loader configuration files are based on the Spring Framework, which is an open-source, full-stack Java/J2EE application framework.

The Spring Framework allows you to use XML files to configure beans. Each bean represents an instance of an object; the parameters correspond to each object's setter methods. A typical bean has the following attributes:

id

Uniquely identifies the bean to `XmlBeanFactory`, which is the class that gets objects from an XML configuration file.

class

Specifies the implementation class for the bean instance.

For more information on the Spring Framework, see the official documentation and the support forums. Note that Salesforce cannot guarantee the availability or accuracy of external websites.

SEE ALSO:

Configure Database Access

Data Access Objects

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Note: The Data Loader command-line interface is supported for Windows only.

When running Data Loader in batch mode from the command line, several data access objects are supported. A data access object allows access to an external data source outside of Salesforce. They can implement a read interface (`DataReader`), a write interface (`DataWriter`), or both. See the following list of object names and descriptions.

csvRead

Allows the reading of a comma or tab-delimited file. There should be a header row at the top of the file that describes each column.

csvWrite

Allows writing to a comma-delimited file. A header row is added to the top of the file based on the column list provided by the caller.

databaseRead

Allows the reading of a database. Use `database-conf.xml` to configure database access.

databaseWrite

Allows writing to a database. Use `database-conf.xml` to configure database access.

SEE ALSO:

Configure Database Access

SQL Configuration

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Note: The Data Loader command-line interface is supported for Windows only.

When running Data Loader in batch mode from the command line, the `SqlConfig` class contains configuration parameters for accessing specific data in the database. As shown in the code samples below, queries and inserts are different but very similar. The bean must be of type `com.salesforce.dataloader.dao.database.SqlConfig` and have the following properties:

`sqlString`

The SQL code to be used by the data access object.

The SQL can contain replacement parameters that make the string dependent on configuration or operation variables. Replacement parameters must be delimited on both sides by "@" characters. For example, `@process.lastRunDate@`.

`sqlParams`

A property of type `map` that contains descriptions of the replacement parameters specified in `sqlString`. Each entry represents one replacement parameter: the key is the replacement parameter's name, the value is the fully qualified Java type to be used when the parameter is set on the SQL statement. Note that "java.sql" types are sometimes required, such as `java.sql.Date` instead of `java.util.Date`. For more information, see the official JDBC API documentation.

`columnNames`

Used when queries (`SELECT` statements) return a JDBC `ResultSet`. Contains column names for the data outputted by executing the SQL. The column names are used to access and return the output to the caller of the `DataReader` interface.

SQL Query Bean Example

```
<bean id="accountMasterSql"
    class="com.salesforce.dataloader.dao.database.SqlConfig"
    singleton="true">
    <property name="sqlString"/>
        <value>
            SELECT distinct
                '012x00000000Ij7' recordTypeId,
                accounts.account_number,
                org.organization_name,
                concat (concat(parties.address1, ' '), parties.address2) billing_address,
                locs.city,
                locs.postal_code,
                locs.state,
                locs.country,
                parties.sic_code
            from
                ar.hz_cust_accounts accounts,
                ar.hz_organization_profiles org,
                ar.hz_parties parties,
                ar.hz_party_sites party_sites,
                ar.hz_locations locs
            where
                accounts.PARTY_ID = org.PARTY_ID
                and parties.PARTY_ID = accounts.PARTY_ID
                and party_sites.PARTY_ID = accounts.PARTY_ID
                and locs.LOCATION_ID = party_sites.LOCATION_ID
                and (locs.last_update_date > @process.lastRunDate@ OR
accounts.last_update_date > @process.lastRunDate@
        </value>
    </property>
    <property name="columNames">
        <list>
            <value>recordTypeId</value>
            <value>account_number</value>
            <value>organization_name</value>
            <value>billing_address</value>
            <value>city</value>
            <value>postal_code</value>
            <value>state</value>
            <value>country</value>
            <value>sic_code</value>
        </list>
    </property>
    <property name="sqlParams">
        <map>
            <entry key="process.lastRunDate" value="java.sql.Date"/>
        </map>
    </property>
</bean>
```

SQL Insert Bean Example

```
<bean id="partiesInsertSql"
    class="com.salesforce.dataloader.dao.database.SqlConfig"
    singleton="true">
    <property name="sqlString"/>
        <value>
            INSERT INTO REP.INT_PARTIES (
            BILLING_ADDRESS, SIC_CODE)
            VALUES (@billing_address@, @sic_code@)
        </value>
    </property>
    <property name="sqlParams"/>
        <map>
```

```
            <entry key="billing_address" value="java.lang.String"/>
            <entry key="sic_code" value="java.lang.String"/>
        </map>
    </property>
</bean>
```

SEE ALSO:

Configure Database Access

Map Columns

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Note: The Data Loader command-line interface is supported for Windows only.

When running Data Loader in batch mode from the command line, you must create a properties file that maps values between Salesforce and data access objects.

1. Create a new mapping file and give it an extension of `.sdl`.
2. Observe the following syntax:
   - On each line, pair a data source with its destination.
   - In an import file, put the data source on the left, an equals sign (=) as a separator, and the destination on the right. In an export file, put the destination on the left, an equals sign (=) as a separator, and the data source on the right.
   - Data sources can be either column names or constants. Surround constants with double quotation marks, as in “sampleconstant”. Values without quotation marks are treated as column names.
   - Destinations must be column names.
   - You may map constants by surrounding them with double quotation marks, as in:

     ```
     "Canada"=BillingCountry
     ```

3. In your configuration file, use the parameter `process.mappingFile` to specify the name of your mapping file.

Note: If your field name contains a space, you must escape the space by prepending it with a backslash (\). For example:

```
Account\ Name=Name
```

Column Mapping Example for Data Insert

The Salesforce fields are on the right.

```
SLA__C=SLA__c
BILLINGCITY=BillingCity
SYSTEMMODSTAMP=
OWNERID=OwnerId
CUSTOMERPRIORITY__C=CustomerPriority__c
ANNUALREVENUE=AnnualRevenue
DESCRIPTION=Description
BILLINGSTREET=BillingStreet
SHIPPINGSTATE=ShippingState
```

Column Mapping Example for Data Export

The Salesforce fields are on the left.

```
Id=account_number
Name=name
Phone=phone
```

Column Mapping for Constant Values

Data Loader supports the ability to assign constants to fields when you insert, update, and export data. If you have a field that should contain the same value for each record, you specify that constant in the `.sdl` mapping file instead of specifying the field and value in the CSV file or the export query.

The constant must be enclosed in double quotation marks. For example, if you're importing data, the syntax is `"constantvalue"=field1`.

If you have multiple fields that should contain the same value, you must specify the constant and the field names separated by commas. For example, if you're importing data, the syntax would be `"constantvalue"=field1, field2`.

Here's an example of an `.sdl` file for inserting data. The Salesforce fields are on the right. The first two lines map a data source to a destination field, and the last three lines map a constant to a destination field.

```
Name=Name
NumEmployees=NumberOfEmployees
"Aerospace"=Industry
"California"=BillingState, ShippingState
"New"=Customer_Type__c
```

A constant must contain at least one alphanumeric character.

Note: If you specify a constant value that contains spaces, you must escape the spaces by prepending each with a backslash (\). For example:

```
"Food\ &\ Beverage"=Industry
```

Run Individual Batch Processes

Note: The Data Loader command-line interface is supported for Windows only.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

To start an individual batch process, use `\bin\process.bat`, which requires the following parameters:

A configuration directory

The default is `\conf`.

To use an alternate directory, create a new directory and add the following files to it:

- If your process is not interactive, copy `process-conf.xml` from `\samples\conf`.
- If your process requires database connectivity, copy `database-conf.xml` from `\samples\conf`.
- Copy `config.properties` from `\conf`.

A process name

The name of the ProcessRunner bean from `\samples\conf\process-conf.xml`.

Process Example

```
process ../conf accountMasterProcess
```

Note: You can configure external process launchers such as the Microsoft Windows XP Scheduled Task Wizard to run processes on a schedule.

Data Loader Command Line Introduction

Note: The Data Loader command-line interface is supported for Windows only.

In addition to using Data Loader interactively to import and export data, you can run it from the command line. You can use commands to automate the import and export of data.

This quick start shows you how to use the Data Loader command-line functionality to import data. Follow these steps.

- Step 1: Create the encryption key
- Step 2: Create the encrypted password for your login username
- Step 3: Create the Field Mapping File
- Step 4: Create a `process-conf.xml` file that contains the import configuration settings
- Step 5: Run the process and import the data

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Prerequisites

Note: The Data Loader command-line interface is supported for Windows only.

To step through this quick start requires the following:

- Data Loader installed on the computer that runs the command-line process.
- The Java Runtime Environment (JRE) installed on the computer that runs the command-line process.
- Familiarity with importing and exporting data by using the Data Loader interactively through the user interface. This makes it easier to understand how the command-line functionality works.

Tip: When you install Data Loader, sample files are installed in the samples directory. This directory is found below the program directory, for example, `C:\Program Files (x86)\salesforce.com\Apex Data Loader 22.0\samples\`. Examples of files that are used in this quick start can be found in the `\samples\conf` directory.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Step One: Create the Encryption Key

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Note: The Data Loader command-line interface is supported for Windows only.

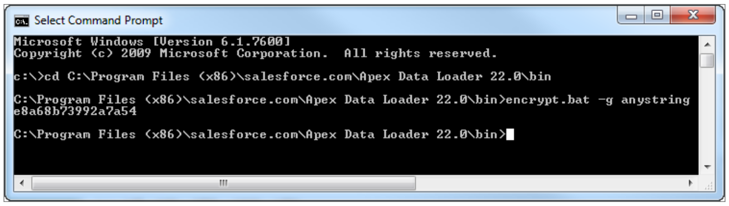
When you use Data Loader from the command line, there's no user interface. Therefore, you provide the information that you would enter in the user interface in a text file named `process-conf.xml`. For example, you add the username and password that Data Loader uses to log in to Salesforce. The password must be encrypted before you add it to the `process-conf.xml` file, and creating the key is the first step in that process.

1. Open a command prompt window by selecting **Start** > **All Programs** > **Accessories** > **Command Prompt**. Alternatively, you can click **Start** > **Run**, enter *`cmd`* in the **Open** field, and click **OK**.
2. In the command window, enter *`cd\`* to navigate to the root directory of the drive where Data Loader is installed.
3. Navigate to the Data Loader `\bin` directory by entering this command. Be sure to replace the file path with the path from your system.

   ```
   cd C:\Program Files (x86)\salesforce.com\Apex Data Loader 22.0\bin
   ```

4. Create an encryption key by entering the following command. Replace <seedtext> with any string.

   ```
   encrypt.bat —g <seedtext>
   ```

   ```
   Microsoft Windows [Version 6.1.7600]
   Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

   c:\>cd C:\Program Files (x86)\salesforce.com\Apex Data Loader 22.0\bin

   C:\Program Files (x86)\salesforce.com\Apex Data Loader 22.0\bin>encrypt.bat -g anystring
   e8a68b73992a7a54

   C:\Program Files (x86)\salesforce.com\Apex Data Loader 22.0\bin>
   ```

   Note: To see a list of command-line options for `encrypt.bat`, type *`encrypt.bat`* from the command line.

5. Copy the generated key from the command window to a text file named `key.txt` and make a note of the file path. In this example, the generated key is `e8a68b73992a7a54`.

   Note: Enabling quick edit mode on a command window can make it easier to copy data to and from the window. To enable quick edit mode, right-click the top of the window and select **Properties**. On the Options tab, select **QuickEdit Mode**.

The encryption utility encrypts passwords but not data. HTTPS with TLS 1.0 or later encrypts data transmitted by the Apex Data Loader.

SEE ALSO:

Step Two: Create the Encrypted Password

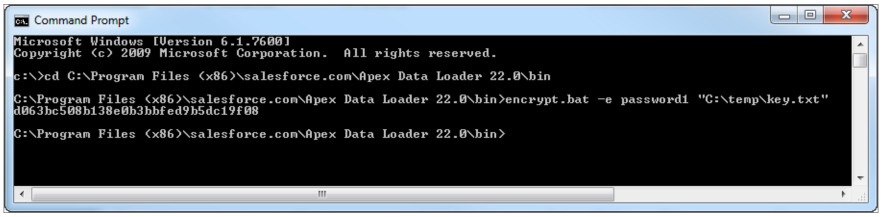
Step Two: Create the Encrypted Password

Note: The Data Loader command-line interface is supported for Windows only.

In this step, you create the encrypted password using the key that you generated in the previous step.

1. In the same command prompt window, enter the following command. Replace <password> with the password that Data Loader uses to log in to Salesforce. Replace <filepath> with the file path to the `key.txt` file that you created in the previous step.

   ```
   encrypt.bat -e <password> "<filepath>\key.txt"
   ```

   ```
   Microsoft Windows [Version 6.1.7600]
   Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

   c:\>cd C:\Program Files (x86)\salesforce.com\Apex Data Loader 22.0\bin

   C:\Program Files (x86)\salesforce.com\Apex Data Loader 22.0\bin>encrypt.bat -e password1 "C:\temp\key.txt"
   d063bc508b138e0b3bbfed9b5dc19f08

   C:\Program Files (x86)\salesforce.com\Apex Data Loader 22.0\bin>
   ```

2. Copy the encrypted password that is generated by the command. You use this value in a later step.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

SEE ALSO:

Step Three: Create the Field Mapping File

Step Three: Create the Field Mapping File

Note: The Data Loader command-line interface is supported for Windows only.

In this step, you create a mapping file with an `.sdl` file extension. In each line of the mapping file, pair a data source with its destination.

1. Copy the following to a text file and save it with a name of `accountInsertMap.sdl`. This is a data insert, so the data source is on the left of the equals sign and the destination field is on the right.

   ```
   #Mapping values
   #Thu May 26 16:19:33 GMT 2011
   Name=Name
   NumberOfEmployees=NumberOfEmployees
   Industry=Industry
   ```

   Tip: For complex mappings, you can use the Data Loader user interface to map source and destination fields and then save those mappings to an `.sdl` file. This is done on the Mapping dialog box by clicking **Save Mapping**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

SEE ALSO:

Step Four: Create the Configuration File

Step Four: Create the Configuration File

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Note: The Data Loader command-line interface is supported for Windows only.

The `process-conf.xml` file contains the information that Data Loader needs to process the data. Each `<bean>` in the `process-conf.xml` file refers to a single process such as an insert, upsert, export, and so on. Therefore, this file can contain multiple processes. In this step, you edit the file to insert accounts into Salesforce.

1. Make a copy of the `process-conf.xml` file from the `\samples\conf` directory. Be sure to maintain a copy of the original because it contains examples of other types of Data Loader processing such as upserts and exports.
2. Open the file in a text editor, and replace the contents with the following XML:

```
<!DOCTYPE beans PUBLIC "-//SPRING//DTD BEAN//EN"
"http://www.springframework.org/dtd/spring-beans.dtd">
<beans>
    <bean id="accountInsert"
        class="com.salesforce.dataloader.process.ProcessRunner"
        singleton="false">
        <description>accountInsert job gets the account record from the CSV file
            and inserts it into Salesforce.</description>
        <property name="name" value="accountInsert"/>
        <property name="configOverrideMap">
            <map>
                <entry key="sfdc.debugMessages" value="true"/>
                <entry key="sfdc.debugMessagesFile"
                    value="C:\DLTest\Log\accountInsertSoapTrace.log"/>
                <entry key="sfdc.endpoint" value="https://servername.salesforce.com"/>
                <entry key="sfdc.username" value="admin@Org.org"/>
                <!--Password below has been encrypted using key file,
                    therefore, it will not work without the key setting:
                    process.encryptionKeyFile.
                    The password is not a valid encrypted value,
                    please generate the real value using the encrypt.bat utility -->
                <entry key="sfdc.password" value="e8a68b73992a7a54"/>
                <entry key="process.encryptionKeyFile"
                    value="C:\DLTest\Command Line\Config\key.txt"/>
                <entry key="sfdc.timeoutSecs" value="600"/>
                <entry key="sfdc.loadBatchSize" value="200"/>
                <entry key="sfdc.entity" value="Account"/>
                <entry key="process.operation" value="insert"/>
                <entry key="process.mappingFile"
                    value="C:\DLTest\Command Line\Config\accountInsertMap.sdl"/>
                <entry key="dataAccess.name"
                    value="C:\DLTest\In\insertAccounts.csv"/>
                <entry key="process.outputSuccess"
                    value="c:\DLTest\Log\accountInsert_success.csv"/>
                <entry key="process.outputError"
                    value="c:\DLTest\Log\accountInsert_error.csv"/>
                <entry key="dataAccess.type" value="csvRead"/>
                <entry key="process.initialLastRunDate"
                    value="2005-12-01T00:00:00.000-0800"/>
            </map>
        </property>
    </bean>
</beans>
```

3. Modify the following parameters in the `process-conf.xml` file. For more information about the process configuration parameters, see Data Loader Process Configuration Parameters on page 444.
   - `sfdc.endpoint`—Enter the URL of the Salesforce instance for your organization; for example, `https://`*`yourInstance`*`.salesforce.com/`.
   - `sfdc.username`—Enter the username Data Loader uses to log in.
   - `sfdc.password`—Enter the encrypted password value that you created in step 2.
   - `process.mappingFile`—Enter the path and file name of the mapping file.
   - `dataAccess.Name`—Enter the path and file name of the data file that contains the accounts that you want to import.
   - `sfdc.debugMessages`—Currently set to `true` for troubleshooting. Set this to `false` after your import is up and running.
   - `sfdc.debugMessagesFile`—Enter the path and file name of the command line log file.
   - `process.outputSuccess`—Enter the path and file name of the success log file.
   - `process.outputError`—Enter the path and file name of the error log file.

   Warning: Use caution when using different XML editors to edit the `process-conf.xml` file. Some editors add XML tags to the beginning and end of the file, which causes the import to fail.

SEE ALSO:

Step Five: Import the Data

Step Five: Import the Data

USER PERMISSIONS	
To insert records:	Create on the record
To update records:	Edit on the record
To upsert records:	Create or Edit on the record
To delete records:	Delete on the record
To hard delete records:	Delete on the record

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Note: The Data Loader command-line interface is supported for Windows only.

Now that all the pieces are in place, you can run Data Loader from the command line and insert some new accounts.

1. Copy the following data to a file name `accountInsert.csv`. This is the account data that you import into your organization.

```
Name,Industry,NumberOfEmployees
Dickenson plc,Consulting,120
GenePoint,Biotechnology,265
Express Logistics and Transport,Transportation,12300
Grand Hotels & Resorts Ltd,Hospitality,5600
```

2. In the command prompt window, enter the following command:

   ```
   process.bat "<file path to process-conf.xml>" <process name>
   ```

   - Replace <file path to process-conf.xml> with the path to the directory containing `process-conf.xml`.
   - Replace <process name> with the process specified in `process-conf.xml`.

   Your command should look something like this:

   ```
   process.bat "C:\DLTest\Command Line\Config" accountInsert
   ```

   After the process runs, the command prompt window displays success and error messages. You can also check the log files: `insertAccounts_success.csv` and `insertAccounts_error.csv`. After the process runs successfully, the `insertAccounts_success.csv` file contains the records that you imported, along with the ID and status of each record. For more information about the status files, see Review Data Loader Output Files on page 439.

Data Loader Third-Party Licenses

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

The following third-party licenses are included with the installation of Data Loader:

Technology	Version Number	License
Apache Jakarta Commons BeanUtils	1.6	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons Collections	3.1	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons Database Connection Pooling (DBCP)	1.2.1	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons Logging	1.0.3	http://www.apache.org/licenses/LICENSE-1.1
Apache Commons Object Pooling Library	1.2	http://www.apache.org/licenses/LICENSE-2.0
Apache Log4j	1.2.8	http://www.apache.org/licenses/LICENSE-2.0
Eclipse SWT	3.452	http://www.eclipse.org/legal/epl-v10.html
OpenSymphony Quartz Enterprise Job Scheduler	1.5.1	http://www.opensymphony.com/quartz/license.action
Rhino JavaScript for Java	1.6R2	http://www.mozilla.org/MPL/MPL-1.1.txt
Spring Framework	1.2.6	http://www.apache.org/licenses/LICENSE-2.0.txt

Note: Salesforce is not responsible for the availability or content of third-party websites.

Undoing an Import

If you import accounts, contacts, leads, or solutions by mistake, your administrator can from Setup, enter *Mass Delete Records* in the Quick Find box, then select **Mass Delete Records** to delete the items you mistakenly imported. View the Using Mass Delete to Undo Imports document for instructions.

The Mass Delete Records tools do not support custom objects. If you import custom objects by mistake in Enterprise, Unlimited, Performance, or Developer Edition, your administrator can use the Data Loader to mass delete the mistakenly imported records. See Perform Mass Deletes on page 437.

SEE ALSO:

- Data Import Wizard
- Import Data Into Salesforce

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

User Permissions Needed
To mass delete data: • Modify All Data

General Importing Questions

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

IN THIS SECTION:

- Can I import data in more than one language?
- How do I perform mass updates to records?
- Can I bulk-assign records to a record type?
- How do I update fields with blank values?
- Can I import using external IDs?
- Can I match lookups and master-detail records using external IDs?
- How many campaign members can I import?
- Who can import campaign members?
- What status is assigned to campaign members?
- Data Import Wizard FAQ

Can I mass upload data into Salesforce?

Group, Professional, Performance, Unlimited, Enterprise, and Developer editions allow you to mass upload data using the Data Import Wizard. From Setup, enter `Data Import Wizard` in the Quick Find box, then select **Data Import Wizard**. In addition, Performance, Unlimited, Enterprise, and Developer editions have API access to use database mass upload tools like Data Loader.

Can I bulk-assign records to a record type?

Yes, you can bulk-assign records to a record type using the Data Import Wizard. You choose to which record type to assign the records during the import process. This process applies to standard and custom objects.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small popup windows, while the Data Import Wizard opens in a full browser with dataimporter.app at the end of the URL. From Setup, enter `Data Import Wizard` in the `Quick Find` box, then select **Data Import Wizard**. The options you see depend on your permissions.

Should I sync Outlook or use import wizards to upload my data into Salesforce?

Use the following information to determine how to upload data into Salesforce.

- To upload accounts and contacts for multiple users at the same time, use the Data Import Wizard and select **Accounts and Contacts**.
- To upload your contacts from any application other than Microsoft Outlook, use the Data Import Wizard and select **Accounts and Contacts**.
- To keep your Outlook contacts, accounts, and calendar events up to date with Salesforce, use Lightning Sync or Salesforce for Outlook to initially sync and update your data.
- To upload custom objects, leads, person accounts, campaign members, and solutions, use the Data Import Wizard and select the appropriate object to import those kinds of records into Salesforce. You can't sync those records using Lightning Sync or Salesforce for Outlook.
- To upload business accounts and contacts for multiple users at the same time, use the Data Import Wizard and select **Accounts and Contacts**.

Note: When you import person accounts, the following limitations apply.

- You can't upload person accounts with Salesforce for Outlook.
- You can sync contacts in Outlook to person accounts in Salesforce only if the person accounts already exist. Syncing doesn't convert Outlook contacts to person accounts in Salesforce.

For more information about importing person accounts, see Data Import Wizard on page 420.

Who can use the Data Import Wizard?

You can use the Data Import Wizard to import accounts, contacts, leads, solutions, person accounts, campaign members, and custom objects for multiple users at the same time. In Personal Edition, the Data Import Wizard isn't available. In Contact Manager Edition, you can't import leads and solutions with the Data Import Wizard. In Group Edition and Essentials Edition, you can't import solutions with the Data Import Wizard.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small popup windows, while the Data Import Wizard opens in a full browser with dataimporter.app at the end of the URL. From Setup, enter `Data Import Wizard` in the `Quick Find` box, then select **Data Import Wizard**. The options you see depend on your permissions.

What permissions do I need to import records?

Data Loader

Importing records with the Data Loader requires these permissions.

- "Read," "Create," "Edit," and "Delete" on the objects
- "API Enabled"
- "Bulk API Hard Delete" (only if you configure Data Loader to use Bulk API to hard-delete records)

Data Import Wizard

Import Option	User Permissions Needed
To import accounts and contacts that you own via the Data Import Wizard:	Import Personal Contacts
To import accounts and contacts owned by others via the Data Import Wizard:	Modify All Data
To import leads via the Data Import Wizard:	Import Leads
To import custom object data via the Data Import Wizard:	Import Custom Objects AND Create on the custom object AND Edit on the custom object
To import solutions via the Data Import Wizard:	Import Solutions
To add or update campaign members via the Data Import Wizard:	**Marketing User** selected in your user information AND Read on contacts OR Import Leads AND

Import Option	User Permissions Needed
	Edit on campaigns
To add contacts that you own to a campaign via the Data Import Wizard:	**Marketing User** selected in your user information AND Create on accounts AND Read on contacts AND Edit on accounts and campaigns AND Import Personal Contacts
To create contacts that you own and add them to a campaign via the Data Import Wizard:	**Marketing User** selected in your user information AND Create on accounts AND Read on contacts AND Edit on accounts and campaigns AND Import Personal Contacts
To add contacts owned by others to a campaign via the Data Import Wizard:	**Marketing User** selected in your user information AND Create on accounts AND Read on contacts AND Edit on accounts, contacts, and campaigns AND Modify All Data
To create contacts owned by others and add them to a campaign via the Data Import Wizard:	**Marketing User** selected in your user information AND Create on accounts AND Read on contacts AND

Import Option	User Permissions Needed
	Edit on accounts, contacts, and campaigns AND Modify All Data
To add existing leads to a campaign via the Data Import Wizard:	**Marketing User** selected in your user information AND Edit on campaigns AND Import Leads
To create leads and add them to a campaign via the Data Import Wizard:	**Marketing User** selected in your user information AND Edit on campaigns AND Import Leads
To add person accounts that you own to a campaign via the Data Import Wizard:	Create on accounts AND Edit on accounts AND Import Personal Contacts
To create person accounts that you own via the Data Import Wizard:	Create on accounts AND Edit on accounts AND Import Personal Contacts
To add person accounts owned by others to a campaign via the Data Import Wizard:	Create on accounts AND Edit on accounts and contacts AND Modify All Data
To create person accounts owned by others via the Data Import Wizard:	Create on accounts AND Edit on accounts and contacts AND Modify All Data

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small popup windows, while the Data Import Wizard opens in a full browser with dataimporter.app at the end of the URL. From Setup, enter `Data Import Wizard` in the `Quick Find` box, then select **Data Import Wizard**. The options you see depend on your permissions.

What file formats can the import wizards handle?

You can import contacts and business accounts directly from an ACT! or Outlook file, or from any CSV (comma-separated values) file, such as a GoldMine or Excel file. You can import leads, solutions, custom objects, or person accounts from any CSV file.

Note: If commas aren't appropriate for your locale, use a tab or other delimiter. Specify your delimiter in Data Loader Settings (**Settings** | **Settings**).

Which data can I import?

You can use import wizards to import the following records.

Campaign Member status

In Professional, Enterprise, Unlimited, Performance, and Developer Edition orgs, use the Data Import Wizard to import the status of campaign members.

Contacts and business accounts

Use the Data Import Wizard to import contacts and business accounts.

In Professional, Enterprise, Unlimited, Performance, and Developer Edition orgs, you can also import contact and business account notes.

Person accounts

In Professional, Enterprise, Unlimited, Performance, and Developer Edition orgs, use the Data Import Wizard to import person accounts.

Leads

In Professional, Enterprise, Unlimited, Performance, and Developer Edition orgs, use the Data Import Wizard to import leads.

Solutions

In Professional, Enterprise, Unlimited, Performance, and Developer Edition orgs, use the Data Import Wizard to import solutions.

Custom objects

In Contact Manager, Group, Professional, Enterprise, Unlimited, Performance, and Developer Edition orgs, use the Data Import Wizard to import custom objects.

You can import values into a field only if you have read and edit access. User permissions, page layout assignments, and field-level security settings determine field access.

Import wizards for other records are not available.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small popup windows, while the Data Import Wizard opens in a full browser with dataimporter.app at the end of the URL. From Setup, enter `Data Import Wizard` in the `Quick Find` box, then select **Data Import Wizard**. The options you see depend on your permissions.

How large can my import file be?

- Your import file can be up to 100 MB, but each record in your file can't exceed 400 KB, which is about 4,000 characters. To determine how many fields you can import, use this formula: 4,000 / (average number of characters in an API field name * 2). For example, if your average field character length is 40, you can import approximately 50 fields.

- You can import up to 90 fields per record.
- Each imported note and each imported description can't exceed 32 KB. Text longer than 32 KB is truncated.
- Other Bulk API limits apply. If you have missing records or truncated fields due to limits, see Bulk API Limits in the Bulk API Developer Guide.

Your import is also subject to your org's storage limit. The size of your import file doesn't directly correlate to the storage space needed for those records. For example, a 50 MB import file might not create 50 MB of data in Salesforce.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small popup windows, while the Data Import Wizard opens in a full browser with dataimporter.app at the end of the URL. From Setup, enter *`Data Import Wizard`* in the `Quick Find` box, then select **Data Import Wizard**. The options you see depend on your permissions.

Why can't I log in to Data Loader?

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

If you're having trouble logging in to Data Loader, try the following solutions.

- Add a security token to the end of your password to log in to Data Loader.
- Change the `Server host` to point to the appropriate server in Data Loader by following these steps:
  1. Start the Data Loader.
  2. Navigate to **Settings** > **Settings**.
  3. Set `Server host` to `https://`*`yourInstance`*`.salesforce.com/`, where *`instance_name`* is the Salesforce instance you're on.
  4. Click **OK** to save your settings.
- Ask your administrator whether you're working behind a proxy server. If so, adjust your Data Loader settings. If you're using APIs that are behind a proxy server, the proxy server prevents the APIs from connecting with Salesforce servers; you won't see information about the APIs under Login History.
- Try to log in on another computer to verify that your local device settings aren't causing the problem.

SEE ALSO:

Reset Your Security Token

Set Trusted IP Ranges for Your Organization

Why isn't Data Loader importing special characters?

If Data Loader fails to import special characters such as ö, ñ, or é, your source data file might not be properly encoded. To ensure the file is properly encoded:

1. Make any modifications to your source data file in .xls format.
2. In Microsoft® Excel®, save a copy of your file as a Unicode Text file.
3. Open the Unicode Text file you just saved with a text editor.
4. Click **File** > **Save As** to change the following file settings:
   - File name extension—*`.csv`*
   - Save as type—**All Files**
   - Encoding—**UTF-8**

5. Click **Save**, and close the file.

   Note: Don’t open the file after you have saved the settings or you may revert the encoding changes.

6. Import the data using Data Loader as you normally would, and select the newly created .csv file.

Can I import into custom fields?

Yes. Your administrator must create the custom fields prior to import.

For checkbox fields, records with a value of *1* in the field are imported as checked, while a value of *0* is not checked.

SEE ALSO:

Import Data Into Salesforce

Can I import into fields that are not on my page layout?

No. You can import values into a field only if you have read and edit access. User permissions, page layout assignments, and field-level security settings determine field access.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small popup windows, while the Data Import Wizard opens in a full browser with dataimporter.app at the end of the URL. From Setup, enter `Data Import Wizard` in the `Quick Find` box, then select **Data Import Wizard**. The options you see depend on your permissions.

Can I import data into a picklist field if the values don’t match?

We recommend that you import your data into an existing picklist when that picklist accurately represents your data, even if the exact values don’t match. The import wizards warn you before importing any new picklist values. However, the wizards accept any value for a picklist field, even if the value isn’t predefined. Your administrator can later edit the picklist to include the needed values. Note that the import wizards don’t allow you to import more than 100 new picklist or multi-select picklist values for any field during a single import.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small popup windows, while the Data Import Wizard opens in a full browser with dataimporter.app at the end of the URL. From Setup, enter `Data Import Wizard` in the `Quick Find` box, then select **Data Import Wizard**. The options you see depend on your permissions.

Can I delete my imported data if I make a mistake?

From Setup, your administrator can enter `Mass Delete Records` in the `Quick Find` box, then select **Mass Delete Records** to perform a mass delete of accounts, contacts, leads, or solutions that you mistakenly imported. You cannot mass delete mistakenly imported custom objects.

View the Using Mass Delete to Undo Imports document for instructions.

How do I use the Data Import Wizard to update records that match specified Salesforce IDs?

You can use the Data Import Wizard to update leads, contacts, or accounts using the record’s ID as the unique identifier. These steps do not apply to custom objects.

Note: These steps assume you have administrator-level of knowledge with Salesforce.

Before you begin, prepare the data you're updating.

1. Create a tabular report for the records you're updating, including the record ID and the fields you're updating.
2. Save the report locally as a .csv file for backup purposes.
3. Click **Save As** to create a new version of the .csv file and make your changes to the data.
4. Click **Save**.

After you have updated the report, import the .csv file into Salesforce. The steps vary based on the records you're updating.

Update Leads

1. From Setup, enter *`Data Import Wizard`* in the Quick Find box, then select **Data Import Wizard**.
2. Click **Launch Wizard**.
3. Select **Leads**, then select **Update existing records**.
4. Set `Match Lead by` to Salesforce.com ID.
5. Select the CSV file that contains your import data, and click **Next**.
6. Map the `Lead ID` field to the Lead ID column in your CSV file, and map the other fields.
7. Click **Next**.
8. Review the import settings, and then click **Start Import**.

Update Accounts or Contacts

1. From Setup, enter *`Data Import Wizard`* in the Quick Find box, then select **Data Import Wizard**.
2. Click **Launch Wizard**.
3. Select **Accounts and Contacts**, then select **Update existing records**.
4. Set `Match Contact by` to Salesforce.com ID.
5. Set `Match Account by` to Salesforce.com ID.
6. Select `Update existing Account information`.
7. Select the CSV file that contains your import data, and click **Next**.
8. Map the contact ID, phone, and address fields to the relevant columns in your CSV file.
9. Map the account ID and other fields to the relevant columns in your CSV file.
10. Click **Next**.
11. Review the import settings, and then click **Start Import**.

The Data Import Wizard matches the record IDs in your file with the record IDs in Salesforce and updates the fields that were mapped.

SEE ALSO:

Data Import Wizard

Why do date fields import incorrectly when I use the Data Loader?

When importing date fields using the Data Loader, sometimes dates import incorrectly because the Data Loader converts the date specified in the imported .csv file to GMT. If your machine's time zone isn't GMT or if your machine's clock adjusts for daylight savings time (DST), your dates may be off by a day.

To prevent the Data Loader from adjusting the date when it converts to GMT, directly change the format of cells containing dates to reflect the native time zone.

1. Open your .csv file in Microsoft® Excel®.
2. In each cell in which you entered dates, add hour data to represent the native time zone. For example, if the date is June 9, 2011 and the time zone is GMT+8, enter *June 9, 2011 8:00*. Excel will reformat this to 6/9/2011 8:00.
3. Right-click the cell in which you entered dates, and click **Format Cells**.
4. Click **Number** > **Custom**.
5. In Type, enter *yyyy-mm-ddThh:mm:ss.sssZ*. For example, if the cell was *6/9/2011 8:00*, it's now 2011-06-09T08:00:00.00Z.

How long does it take to import a file?

For the individual user import wizard, the length of time required depends on the amount of data, but on average it takes only a few minutes.

The administrator import wizards work asynchronously, and you receive a notification email after your file has been successfully imported. The asynchronous import can take a few minutes to no more than 24 hours.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small popup windows, while the Data Import Wizard opens in a full browser with dataimporter.app at the end of the URL. From Setup, enter *Data Import Wizard* in the Quick Find box, then select **Data Import Wizard**. The options you see depend on your permissions.

Why might there be a delay in importing my file?

To manage the volume of imports and ensure that all users receive the highest level of performance, org import files are accepted in asynchronous mode. This means that your file passes through a controlled queue and is imported when the system can best manage the data, however your org import doesn't take longer than 24 hours to complete. You receive a notification email when the import is complete.

Can I import amounts in different currencies?

If your Group, Professional, Enterprise, Unlimited, Performance, or Developer Edition org has set up the ability to use multiple currencies, you can import amounts in different currencies using the Currency ISO Code column in your import file.

Can Customer Support help me import my data?

Customer Support is available to assist Group, Contact Manager, Professional, Enterprise, Unlimited, and Performance Edition orgs throughout the import process.

Can I import data in more than one language?

The import wizard imports one language at a time, the language of the user doing the import. If you have the same data in different languages, run an import for each additional language.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small popup windows, while the Data Import Wizard opens in a full browser with dataimporter.app at the end of the URL. From Setup, enter *`Data Import Wizard`* in the `Quick Find` box, then select **Data Import Wizard**. The options you see depend on your permissions.

How do I perform mass updates to records?

To update more than 50,000 records but less than 5 million records, use Data Loader.

To update more than 5 million records, we recommend you work with a Salesforce partner or visit the *App Exchange* for a suitable partner product.

Can I bulk-assign records to a record type?

Yes, you can bulk-assign records to a record type using the Data Import Wizard. You choose to which record type to assign the records during the import process. This process applies to standard and custom objects.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the Data Import Wizard. Individual import wizards open in small popup windows, while the Data Import Wizard opens in a full browser with dataimporter.app at the end of the URL. From Setup, enter *`Data Import Wizard`* in the `Quick Find` box, then select **Data Import Wizard**. The options you see depend on your permissions.

How do I update fields with blank values?

To replace fields with null values, you must use Data Loader.

1. Choose **Start** > **All Programs** > **Salesforce** > **Data Loader** > **Data Loader** to open Data Loader.
2. Click **Export** and complete the wizard. When the operation finishes, click **View Extraction**.
3. Click **Open in external program** to open your data in Excel. Blank out the fields you want to update.
4. In Data Loader, choose **Settings** > **Settings**, and select **Insert null values**. Click **OK** to save your settings.
5. Click **Update** and follow the wizard to reimport your data.

Can I import using external IDs?

When importing custom objects, solutions, or person accounts, you can use external IDs to prevent the import from creating duplicate records.

An external ID is a custom field that has the External ID attribute, meaning that it contains unique record identifiers from a system outside of Salesforce. When you select this option, the Data Import Wizard detects existing records in Salesforce with external IDs that match those values in the import file.

Can I match lookups and master-detail records using external IDs?

Yes, using the Data Import Wizard, you can choose from multiple external IDs to match to lookups and master-detail records.

How many campaign members can I import?

With the Data Import Wizard, your import file can have up to 50,000 record rows. Your imports are also subject to the overall storage limits for your org.

Who can import campaign members?

Only users with the required permissions can import campaign members with the Data Import Wizard.

Import Option	User Permissions Needed
To add or update campaign members via the Data Import Wizard:	**Marketing User** selected in your user information AND Read on contacts OR Import Leads AND Edit on campaigns
To add contacts that you own to a campaign via the Data Import Wizard:	**Marketing User** selected in your user information AND Create on accounts AND Read on contacts AND Edit on accounts and campaigns AND Import Personal Contacts
To create contacts that you own and add them to a campaign via the Data Import Wizard:	**Marketing User** selected in your user information AND Create on accounts AND Read on contacts AND Edit on accounts and campaigns AND Import Personal Contacts
To add contacts owned by others to a campaign via the Data Import Wizard:	**Marketing User** selected in your user information AND Create on accounts AND Read on contacts

Import Option	User Permissions Needed
	AND Edit on accounts, contacts, and campaigns AND Modify All Data
To create contacts owned by others and add them to a campaign via the Data Import Wizard:	**Marketing User** selected in your user information AND Create on accounts AND Read on contacts AND Edit on accounts, contacts, and campaigns AND Modify All Data
To add existing leads to a campaign via the Data Import Wizard:	**Marketing User** selected in your user information AND Edit on campaigns AND Import Leads
To create leads and add them to a campaign via the Data Import Wizard:	**Marketing User** selected in your user information AND Edit on campaigns AND Import Leads
To add person accounts that you own to a campaign via the Data Import Wizard:	Create on accounts AND Edit on accounts AND Import Personal Contacts
To add person accounts owned by others to a campaign via the Data Import Wizard:	Create on accounts AND Edit on accounts and contacts AND Modify All Data

What status is assigned to campaign members?

With the Data Import Wizard, you can map a column in your import file to the `Status` field. Blank or invalid status values are set to the default status.

Data Import Wizard FAQ

IN THIS SECTION:

- How many records can I import?
- What kind of objects can I import?
- Can I do simultaneous imports?
- How long does it take to complete an import?

SEE ALSO:

- Data Import Wizard

How many records can I import?

The Data Import Wizard lets you import up to 50,000 records at a time.

SEE ALSO:

- Data Import Wizard FAQ

What kind of objects can I import?

You can use the Data Import Wizard to import accounts, contacts, leads, solutions, campaign members, person accounts, and custom objects.

SEE ALSO:

- Data Import Wizard FAQ

Can I do simultaneous imports?

The Data Import Wizard doesn't support simultaneous—or concurrent—data import jobs, even from separate browser windows. Finish one data import before beginning the next.

SEE ALSO:

- Data Import Wizard FAQ

How long does it take to complete an import?

The time it takes to complete an import using the Data Import Wizard varies, depending on the amount of data you're importing. Imports are generally not immediate and can take up to several minutes.

If you're a Salesforce admin, you can check the status of an import on the Bulk Downloads page. From Setup, enter *`Bulk Data Load Jobs`* in the `Quick Find` box, then select **Bulk Data Load Jobs**.

If you're not a Salesforce admin and you want to know the status of an import, you need to wait until you receive the status email. You can also monitor the import manually by checking the relevant tabs in Salesforce.

SEE ALSO:

Data Import Wizard FAQ

Export Backup Data from Salesforce

Your Salesforce org can generate backup files of your data on a weekly or monthly basis depending on your edition. You can export all your org's data into a set of comma-separated values (CSV) files.

Note: Users with the "Weekly Data Export" permission can view all exported data and all custom objects and fields in the Export Service page. This permission is granted by default only to the System Administrator profile because it enables wide visibility.

You can generate backup files manually once every 7 days (for weekly export) or 29 days (for monthly export). In Professional Edition and Developer Edition, you can generate backup files only every 29 days. You can schedule backup files to generate automatically at weekly or monthly intervals (only monthly intervals are available in Professional Edition and Developer Edition).

Heavy traffic can delay an export delivery. For example, assume that you schedule a weekly export to run until the end of the month, beginning April 1. The first export request enters the queue, but due to heavy traffic, the export isn't delivered until April 8. On April 7, when your second export request is scheduled to be processed, the first request is still in the queue. So, the second request isn't processed until April 14.

Note: Only active users can run export jobs. If an inactive user schedules an export, error emails are generated and the export doesn't run.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Weekly export available in: **Enterprise**, **Performance**, and **Unlimited** Editions

Monthly export available in: **All** editions, except for Database.com

USER PERMISSIONS

To export data:
- Weekly Data Export

1. From Setup, enter *`Data Export`* in the `Quick Find` box, then select **Data Export** and **Export Now** or **Schedule Export**.
   - The **Export Now** option prepares your files for export immediately. This option is only available if enough time has passed since your last export.
   - The **Schedule Export** option allows you to schedule the export process for weekly or monthly intervals.
2. Select the desired encoding for your export file.
3. Select `Include images, documents, and attachments` and `Include Chatter files and Salesforce CRM Content document versions` to include these items in your export data.

   Note: Including special content in the export increases data export processing time.
4. If you want to have spaces instead of carriage returns or line breaks in your export files, select `Replace carriage returns with spaces`. This selection is useful if you plan to use your export files for importing or other integrations.
5. If you're scheduling your export, select the frequency (only available for orgs with monthly exports), start and end dates, and time of day for your export.
6. Under Exported Data, select the types of data to include in your export. If you aren't familiar with the terminology used for some of the types of data, we recommend that you select **Include all data**. Note the following:

- Formula and roll-up summary fields are always excluded from exports.
- If your org uses divisions, data from all divisions is included in the export.
- If your org uses person accounts and you are exporting accounts, all account fields are included in the account data.
- If your org uses person accounts and you are exporting contacts, person account records are included in the contact data. However, the contact data only includes the fields shared by contacts and person accounts.
- For information on field limitations, see the *Salesforce Field Reference Guide*.

7. Click **Start Export** or **Save**.

   Salesforce creates a zip archive of CSV files and emails the user who scheduled the export when it's ready. The email address for this notification can't be changed. Exports complete as soon as possible, however we can't guarantee the date and time of completion. Large exports are broken up into multiple files. To download the zip file, follow the link in the email or click **Data Export**. Zip files are deleted 48 hours after the email is sent.

   Note: For security purposes, Salesforce can require users to pass a CAPTCHA user verification test to export data from their org. This simple text-entry test prevents malicious programs from accessing your org's data. To pass the test, users must correctly type the two words displayed in the overlay's text box. The words entered in the text box must be separated by a space.

Tip: Ensure that any automated processes that process the export files rely on the column headings in the CSV files, rather than the position of the columns.

Backup Data Export Considerations

No Sandbox Support

The data export service isn't supported in sandboxes. You can request an export in your sandbox, but the export doesn't get processed and doesn't complete. The only way to remove the export request after it's been queued is to refresh your sandbox.

File Size Considerations

If the size of data in the org is large, multiple .zip archives are created. Each .zip archive file contains one or more .csv files and can be up to 512 MB (approximately). If the total size of exported data is greater than 512 MB, the export generates multiple .zip files.

Adjust Export Files

Depending on the encoding selected, you might have to make adjustments to the export file before viewing it. Use the following instructions that apply to the character encoding you selected.

- View Unicode (UTF-8) Encoded Export Files
- View Unicode (UTF-16, Big Endian) Encoded Export Files
- View Unicode (Little Endian) Encoded Export Files

View Unicode (UTF-8) Encoded Export Files

If you have Microsoft Excel 2003:

1. Open Microsoft Excel.
2. Click **File** > **New**.
3. Click **Data** > **Import External Data** > **Import Data**.
4. In the Microsoft Excel text import wizard, select the CSV file.

5. Select "Delimited" and choose the "Unicode (UTF-8)" option for File origin.
6. Click **Next**.
7. Select `Comma` in the Delimiters section and click **Finish**. You might be prompted to select a range of cells.

   Note: If commas aren't appropriate for your locale, use a tab or other delimiter. Specify your delimiter in Data Loader Settings (**Settings** | **Settings**).

8. Repeat these steps for each file.

If you have an earlier version of Microsoft Excel (pre-2003):

1. Open the file in Microsoft Excel.
2. Select **File** > **Save As**.
3. Save the file as type Web Page.
4. Select **Tools** > **Options** > **General** tab and click the **Web Options** button.
5. Select the Encoding tab, and then choose the "Unicode (UTF-8)" option.
6. To close the dialog boxes, click **OK**.
7. To save the file with selected encoding, select **File** > **Save**.
8. Repeat these steps for each file.

View Unicode (UTF-16, Big Endian) Encoded Export Files

Open the export files in a text editor that supports this character set. Microsoft Excel does not support this character set.

View Unicode (Little Endian) Encoded Export Files

1. Open the file in Microsoft Excel.
2. Click column A to highlight the entire first column.
3. Open the **Data** menu and choose **Text to Columns**.
4. Select the "Delimited" radio button and click **Next**.
5. Select "Comma" in the Delimiters section and click **Finish**.

   Note: If commas aren't appropriate for your locale, use a tab or other delimiter. Specify your delimiter in Data Loader Settings (**Settings** | **Settings**).

6. Repeat these steps for each file.

Transferring Records

A record owner, or any user above the owner in the role or territory hierarchy, can transfer a single record to another user. With some objects, like cases, leads, and campaigns, a user may be granted access to transfer records through sharing. Depending on the type of object, there may be multiple ways to transfer records to another user:

Method	Available for
Transfer a single record	Accounts, campaigns, cases, contacts, contracts, leads, and custom objects
Transfer multiple records by selecting the records from a list view and clicking **Change Owner**	Cases, leads, and custom objects, which can belong to either a user or a queue
Transfer multiple records using the Mass Transfer tool	Accounts, leads, and custom objects

Ability to Change Ownership

- Users with the "Modify All Data" permission, or users with the "Modify All" permission for the given object, can transfer any record, regardless of who owns the record.
- To transfer a single record or multiple records from a list view, the new owner must have at least the "Read" permission on the object type. This rule does not apply if you use the mass transfer tool.
- To transfer ownership of any single record in an organization that does not use territory management, a user must have the appropriate "Edit" permission and either own the record or be above the owner in the role hierarchy.

  For example, to transfer ownership of an account, a user must have "Read" and "Edit" access to the account. Additionally, the new owner of the record must have at least "Read" permission on accounts.

  The Public Full Access and Public Read/Write/Transfer sharing settings give all users the ability to transfer ownership of that type of record as long as they have the appropriate "Edit" permission.
- In organizations that use territory management, users that have been assigned to territories can be enabled to transfer the accounts in their territories, even if they are not the record owner.
- To transfer campaigns, users must also have the `Marketing User` checkbox selected on their user record.

Changing Ownership for Portal Accounts

- To transfer a Partner account, you must have the "Manage Users" or "Manage External Users" permission.
- If you are the owner of a Customer Portal account and want to transfer the account, you can transfer the account to any user in your same role without the need for special permission. You cannot transfer a Customer Portal account to a user with a higher or lower role.

EDITIONS

Available in: Salesforce Classic

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

Accounts, Campaigns, Contacts, Contracts, Leads, and Cases are not available in **Database.com**.

Contracts are available in: **Performance** and **Developer** Editions and in **Professional**, **Enterprise**, and **Unlimited** Editions with the Sales Cloud.

USER PERMISSIONS

To transfer multiple accounts, campaigns, contacts, contracts, and custom objects:

- Transfer Record

  AND

  Edit on the object type

To transfer multiple leads:

- Transfer Leads OR Transfer Record

  AND

  Edit on leads

To transfer multiple cases:

- Transfer Cases OR Transfer Record

  AND

  Edit on cases

- Partner accounts can only be transferred to users with the “Manage External Users” permission.
- To transfer a Portal account with both Customer and Partner Portal users, you must have the “Manage Users” permission.
- You cannot assign an account with Customer Portal users to an owner who is a partner user.

SEE ALSO:

Mass Transfer Records

Mass Transfer Records

Use the Mass Transfer tool to transfer multiple accounts, leads, service contracts, and custom objects from one user to another.

Note: To transfer any records that you do not own, you must have the required user permissions as well as read sharing access on the records.

1. From Setup, enter *`Mass Transfer Records`* in the `Quick Find` box, then select **Mass Transfer Records**.
2. Click the link for the type of record to transfer.
3. Optionally, fill in the name of the existing record owner in the `Transfer from` field. For leads, you can transfer from users or queues.
4. In the `Transfer to` field, fill in the name of new record owner. For leads, you can transfer to users or queues.
5. If your organization uses divisions, select the `Change division....` checkbox to set the division of all transferred records to the new owner's default division.
6. When transferring accounts, you can:
   - Select `Transfer open opportunities not owned by the existing account owner` to transfer open opportunities owned by other users that are associated with the account.
   - Select `Transfer closed opportunities` to transfer closed opportunities associated with the account. This option applies only to closed opportunities owned by the account owner; closed opportunities owned by other users are not changed.
   - Select `Transfer open cases owned by the existing account owner` to transfer open cases that are owned by the existing account owner and associated with the account.
   - Select `Transfer closed cases` to transfer closed cases that are owned by the existing account owner and associated with the account.
   - Select `Keep Account Team` to maintain the existing account team associated with the account. Deselect this checkbox if you want to remove the existing account team associated with the account.
   - Select `Keep Opportunity Team on all opportunities` to maintain the existing team on opportunities associated with this account. Any opportunity splits are preserved, and split percentages assigned to the previous owner transfer to the new one. If this box is unchecked, all opportunity team members and splits are deleted when the opportunity is transferred.

     Note: If you transfer closed opportunities, the opportunity team is maintained, regardless of this setting.
7. Enter search criteria that the records you are transferring must match. For example, you could search accounts in California by specifying *`Billing State/Province equals CA`*.
8. Click **Find**.
9. Select the checkbox next to the records you want to transfer. To select all currently displayed items, check the box in the column header.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Service Contracts available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions with the Service Cloud

Accounts and Leads not available in: **Database.com**

USER PERMISSIONS

To mass transfer accounts and service contracts:

- Transfer Record

  AND

  Edit on the object type

  AND

  Transfer Leads

To mass transfer custom objects:

- Transfer Record

  AND

  Edit on the object type

To mass transfer leads:

- Transfer Leads OR Transfer Record

  AND

  Edit on leads

Note: If duplicate records are found, you must select only one of the records to transfer. Transferring duplicate records results in an error.

Duplicate records may display if you filter leads based on Campaign Member Status and a matching lead has the same campaign member status on multiple campaigns. For example, if you specify `Campaign Member Status equals Sent`, and a matching lead named John Smith has the status Sent on two campaigns, his record will display twice.

10. Click **Transfer**.

Transfer of Associated Items

When you change record ownership, some associated items that are owned by the current record owner are also transferred to the new owner.

Record	Associated items that are also transferred
Accounts	Contacts (on business accounts only), attachments, notes, open activities, open opportunities owned by the current account owner, and optionally, closed opportunities and open opportunities owned by other users.
Leads	Open activities. When transferring leads to a queue, open activities are not transferred.

Access to Transferred Items

When transferring accounts and their related data in Professional, Enterprise, Unlimited, Performance, and Developer Editions, all previous access granted by manual sharing, Apex managed sharing, or sharing rules is removed. New sharing rules are then applied to the data based on the new owner. The new owner may need to manually share the transferred accounts and opportunities as necessary to grant access to certain users.

SEE ALSO:

Transferring Records

Delete Multiple Records and Reports

You can delete multiple reports or records at the same time.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **All** Editions

This feature is only available in **Database.com** via the API. You can only mass delete records of custom objects in **Database.com**.

USER PERMISSIONS

To mass delete data:

- Modify All Data

The record types you can mass-delete include cases, solutions, accounts, contacts, leads, products, and activities.

Here are some ways that mass delete is handy.

- You've identified multiple reports that are no longer used and you want to unclutter the list of reports on the Reports tab.
- You imported your leads incorrectly and you want to start over.
- A user who recently left your company had contacts that were duplicates of other users' data and you want to delete these duplicate contacts.
- You used to enter leads as accounts with the `Type` field set to Prospect. You now want to convert these accounts into leads.

  Tip: Run a report of these accounts, export it to Excel, and then use the Import Leads wizard to import the data as leads. Then using mass delete, select accounts as the record type to delete and enter *`Type equals Prospect`* to locate all accounts you want to delete.

- You want to delete all the leads that have been converted for your org. Select the lead record type, enter *`Converted equals 1`* for the search criteria, and then click **Search**.
- You want to clean up web-generated leads that were created incorrectly or delete accounts and contacts with whom you no longer do business.

1. We strongly suggest you run a report to archive your information and export your data weekly. See Export Backup Data from Salesforce on page 479.
2. From Setup, enter *`Mass Delete Records`* in the `Quick Find` box, then select **Mass Delete Records** and click the link for the type of record to delete.
3. Review the information that is deleted with the records.
4. Specify conditions that the selected items must match, for example, "State equals California."
5. If you're deleting accounts, specify whether you want to delete accounts with attached closed/won opportunities or attached opportunities owned by others.
6. If you're deleting products, select **Archive Products** if you also want to delete products that are on opportunities.

   This option:

   - Deletes products that are not on opportunities and moves them to the Recycle Bin.
   - Archives products that are on opportunities. These products are not moved to the Recycle Bin and cannot be recovered.

   To delete only those products that are not on opportunities, do not select Archive Products. Selected products that are on opportunities remain checked after the deletion to indicate that they were not included in the deletion.

7. To find records that match, click **Search** and select the items you want to delete. To select all currently displayed items, check the box in the column header.
8. To permanently delete records, select **Permanently delete the selected records**.

   Important: Selecting this option prevents you from recovering the selected records from the Recycle Bin.

9. Click **Delete**.

If you did not select **Permanently delete the selected records**, deleted items are moved to the Recycle Bin.

SEE ALSO:

Notes on Using Mass Delete
Undoing an Import
Using Mass Delete to Undo Imports

Notes on Using Mass Delete

Consider the following when using mass delete:

EDITIONS

Available in: Salesforce Classic

Available in: **All** Editions

This feature is only available in **Database.com** via the API. You can only mass delete records of custom objects in **Database.com**.

USER PERMISSIONS

To mass delete data:
- Modify All Data

General Notes About Mass-Deleting

- You can delete up to 250 items at one time.
- When you delete a record, any associated records that display on that record's related lists are also deleted.
- Only reports in public report folders can be mass-deleted.
- You can't mass-delete reports that are attached to dashboards, scheduled, or used in reporting snapshots.

Notes About Mass Delete for Sales Teams

- You can't delete partner accounts that have partner users.
- Products on opportunities cannot be deleted, but they can be archived.
- When you mass-delete products, all related price book entries are deleted with the deleted products.
- When you delete activities, any archived activities that meet the conditions are also deleted.
- When you delete activities, requested meetings aren't included in the mass-delete until they are confirmed and automatically converted to events.
- When you delete recurring events, their child events are not displayed in the list of possible items to delete, but they are deleted.

Notes About Mass Delete for Service Teams

- Accounts and contacts associated with cases cannot be deleted.
- Contacts enabled for Self-Service, and their associated accounts, cannot be deleted.
- Deleting a master solution does not delete the translated solutions associated with it. Instead, each translated solution becomes a master solution.
- Deleting a translated solution removes the association with its master solution.

Mass Update Addresses

When your data is consistent, your reports and related metrics are more accurate and easier to understand. For example, having different abbreviations for a country or state can skew your data. To make your addresses consistent, you can update country and state/province information in existing fields at one time.

You can mass update addresses in contacts, contracts, and leads.

Tip: To ensure data consistency in new records, consider using state and country picklists.

1. From Setup, enter `Mass Update Addresses` in the `Quick Find` box, then select **Mass Update Addresses**.
2. Select **Countries** or **State/Province**. If you chose State/Province, enter the country in which to update the state or province.
3. Click **Next**.
4. Select the values to update and click **Add**. The Selected Values box displays the values to update.

   The Available Values box displays the address values found in existing records. To find more addresses to update, enter all or part of a value and click **Find**.

   If your organization has large amounts of data, instead of using the Available Values box, enter existing values to update in the text area. Separate each value with a new line.
5. In the **Replace selected values with** field, enter the value with which to replace the specified address data, and click **Next**. If your organization has large amounts of data, this field is called **Replace entered values with**.

   The number and type of address records to update are displayed. If you have large amounts of data, only the values to update are displayed.
6. Click **Replace** to update the values.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To mass update addresses:
- Modify All Data

To mass update addresses of contracts:
- Modify All Data

  AND

  Activate Contracts

SEE ALSO:

Let Users Select State and Country from Picklists

Tips for Mass Updating Addresses

Scalability FAQ

- How scalable is Salesforce?
- Will I see a degradation in performance as Salesforce's subscriber base grows?

How scalable is Salesforce?

The service has the capacity to scale to the largest of teams. The architecture behind the service was designed to handle millions of users. We scale as rapidly as our customers require.

Will I see a degradation in performance as Salesforce's subscriber base grows?

No. We are very conscious of performance and have designed the service to be scalable in such a way that we can constantly stay ahead of customer demand. Our architecture allows us to easily add web and application servers to accommodate more users. The system architecture also allows us to add more database servers as needed to accommodate more users. In addition, the facility that houses our servers provides us with guaranteed bandwidth, which we can increase as needed.

Cache Force.com Data

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

To use Platform Cache, first set up partitions using the Platform Cache Partition tool in Setup. Once you've set up partitions, you can add, access, and remove data from them using the Platform Cache Apex API.

Use Platform Cache partitions to improve the performance of your applications. Partitions allow you to distribute cache space in the way that works best for your applications. Caching data to designated partitions ensures that it's not overwritten by other applications or less-critical data.

To access the Partition tool in Setup, enter *`Platform Cache`* in the `Quick Find` box, then select **Platform Cache**.

Use the Platform Cache Partition tool to:

- Request trial cache.
- Create, edit, or delete cache partitions.
- Allocate the session cache and org cache capacities of each partition to balance performance across apps.
- View a snapshot of the org's current cache capacity, breakdown, and partition allocations (in KB or MB).
- View details about each partition.
- Make any partition the default partition.

To use Platform Cache, create at least one partition. Each partition has one session cache and one org cache segment and you can allocate separate capacity to each segment. Session cache can be used to store data for individual user sessions, and org cache is for data that any users in an org can access. You can distribute your org's cache space across any number of partitions. Session and org cache allocations can be zero, or five or greater, and they must be whole numbers. The sum of all partition allocations, including the default partition, equals the Platform Cache total allocation. The total allocated capacity of all cache segments must be less than or equal to the org's overall capacity.

You can define any partition as the default partition, but you can have only one default partition. When a partition has no allocation, cache operations (such as get and put) are not invoked, and no error is returned.

Capacity calculations occur every 5 minutes by default. To make sure you're seeing the latest capacity and allocation, click **Recalculate**.

IN THIS SECTION:

Request a Platform Cache Trial
To test performance improvements by using Platform Cache in your own org, you can request trial cache for your production org. Enterprise, Unlimited, and Performance editions come with some cache, but adding more cache often provides greater performance. When your trial request is approved, you can allocate capacity to partitions and experiment with using the cache for different scenarios. Testing the cache on a trial basis lets you make an informed decision about whether to purchase cache.

Purchase Platform Cache
You can purchase Platform Cache space to improve the performance of your application.

SEE ALSO:

Apex Developer Guide

Request a Platform Cache Trial

To test performance improvements by using Platform Cache in your own org, you can request trial cache for your production org. Enterprise, Unlimited, and Performance editions come with some cache, but adding more cache often provides greater performance. When your trial request is approved, you can allocate capacity to partitions and experiment with using the cache for different scenarios. Testing the cache on a trial basis lets you make an informed decision about whether to purchase cache.

Salesforce approves trial cache requests immediately and sends you an email to notify you that your Platform Cache trial is active. It can take a few minutes for you to receive the email. You receive 30 MB of trial cache space (10 MB if you have Developer Edition). If you need more trial cache space, contact Salesforce.

Note: You can make up to 10 trial cache requests, and you must wait 90 days between trials.

After you request trial cache, you receive emails at the following intervals.

At activation

You can now allocate capacity to partitions and test the trial cache in your org.

Three days before expiration

Before expiration, be sure to reconfigure your partitions to deallocate the added trial space.

At expiration

The trial cache is removed from your org.

Note: If you haven't deallocated enough space, Salesforce reduces your partition sizes to remove the granted trial cache space.

Developer Edition Orgs

You can request trial cache for a Developer Edition org. After you sign up for the org, request trial cache from the Platform Cache Partition tool. ISVs who are using Developer Edition orgs to create managed packages can get 10 MB of trial cache for up to two Developer Edition orgs. ISVs can contact their Salesforce representative to get trial cache in Developer Edition orgs.

Cache Reduction Algorithm

At the end of your trial period, Salesforce removes the granted trial cache space from your org. Before your trial ends, make sure that you've deallocated your trial cache space. You can deallocate space from the Platform Cache Partition tool by resetting partition allocations. If you don't deallocate the cache space, Salesforce removes the granted cache using the following process.

- The system removes cache from the smallest non-default partition first.

  Note: The size of a partition is the total allocation for the partition, which includes org-wide cache and namespace-specific cache.

- The system then works its way through the partitions from smallest to largest in size. If multiple partitions have the same size, the system proportionally removes cache from these partitions.
- The system reduces partitions to a minimum size of 5 MB, unless all the trial cache space can't be removed. In this case, partitions are reduced to 0 MB.
- The default partition (if it exists) is reduced last only if the trial cache space can't be removed from all other partitions.

If unallocated space is present:

- If the amount of unallocated space is greater than the amount of space that must be removed, the system removes only unallocated space.

- If the amount of unallocated space is less than the amount of space that must be removed, the system removes the unallocated space first. The system then follows the cache reduction process to remove the remaining amount.

SEE ALSO:

Cache Force.com Data

Purchase Platform Cache

You can purchase Platform Cache space to improve the performance of your application.

Platform Cache is available to customers with Enterprise Edition orgs and above. The following editions come with some default cache space, but often, adding more cache gives even greater performance enhancements.

- Enterprise Edition (10 MB by default)
- Unlimited Edition (30 MB by default)
- Performance Edition (30 MB by default)

To determine how much cache would be beneficial to your applications, you can request trial cache and try it out in your org. Platform Cache can improve performance in the following situations, among many others.

- Orgs with a large amount of Apex customization
- Orgs with large numbers of concurrent users
- Orgs or applications with complex calculations or queries

In addition, ISVs can purchase cache for use with the applications they provide to customers.

Cache space is sold in 10-MB blocks, with an annual subscription. To purchase Platform Cache, contact your Salesforce representative.

SEE ALSO:

Cache Force.com Data

Protect Your Salesforce Organization

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

IN THIS SECTION:

Salesforce Security Basics

The Salesforce security features help you empower your users to do their jobs safely and efficiently. Salesforce limits exposure of data to the users that act on it. Implement security controls that you think are appropriate for the sensitivity of your data. We'll work together to protect your data from unauthorized access from outside your company and from inappropriate usage by your users.

Strengthen Your Data's Security with Shield Platform Encryption

Shield Platform Encryption gives your data a whole new layer of security while preserving critical platform functionality. It enables you to encrypt sensitive data at rest, and not just when transmitted over a network, so your company can confidently comply with privacy policies, regulatory requirements, and contractual obligations for handling private data.

Session Security

After logging in, a user establishes a session with the platform. Use session security to limit exposure to your network when a user leaves the computer unattended while still logged in. Session security also limits the risk of internal attacks, such as when one employee tries to use another employee's session. Choose from several session settings to control session behavior.

Activations

Activation tracks information about devices from which users have verified their identity. Salesforce prompts users to verify their identity when they access Salesforce from an unrecognized browser or application. Identity verification adds an extra layer of security on top of username and password authentication. The Activations page lists the login IP addresses and client browsers used.

Authenticate Users

Authentication means preventing unauthorized access to your organization or its data by making sure each logged in user is who they say they are.

Transaction Security

Transaction Security is a framework that intercepts real-time Salesforce events and applies appropriate actions and notifications based on security policies you create. Transaction Security monitors events according to the policies that you set up. These policies are applied against events in your org and specify actions to take when certain event combinations occur. When a policy is triggered, you can have an action taken and receive an optional notification.

Single Sign-On

Single sign-on (SSO) lets users access authorized network resources with one login. You validate usernames and passwords against your corporate user database or other client app rather than Salesforce managing separate passwords for each resource.

My Domain

Add a subdomain to your Salesforce org URL with the My Domain Salesforce feature. Having a subdomain lets you highlight your brand and makes your org more secure. A subdomain is convenient and allows you to personalize your login page.

App Launcher

The App Launcher is how users switch between apps. It displays tiles that link to a user's available Salesforce, connected (third-party), and on-premises apps. You can determine which apps are available to which users and the order in which the apps appear. You can also make the App Launcher the default landing page when users first open Salesforce.

Configure File Upload and Download Security Settings

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

Certificates and Keys

Salesforce certificates and key pairs are used for signatures that verify a request is coming from your organization. They are used for authenticated SSL communications with an external web site, or when using your organization as an Identity Provider. You only need to generate a Salesforce certificate and key pair if you're working with an external website that wants verification that a request is coming from a Salesforce organization.

Salesforce Security Basics

The Salesforce security features help you empower your users to do their jobs safely and efficiently. Salesforce limits exposure of data to the users that act on it. Implement security controls that you think are appropriate for the sensitivity of your data. We'll work together to protect your data from unauthorized access from outside your company and from inappropriate usage by your users.

IN THIS SECTION:

Phishing and Malware

Trust starts with transparency. That's why Salesforce displays real-time information on system performance and security on the trust site at http://trust.salesforce.com. This site provides live data on system performance, alerts for current and recent phishing and malware attempts, and tips on best security practices for your organization.

Security Infrastructure

Salesforce utilizes some of the most advanced technology for Internet security available today. When you access the application using a Salesforce-supported browser, Transport Layer Security (TLS) technology protects your information using both server authentication and Classic Encryption, ensuring that your data is safe, secure, and available only to registered users in your organization.

Security Health Check

As an admin, you can use Health Check to identify and fix potential vulnerabilities in your security settings, all from a single page. A summary score shows how your org measures against a security baseline, like the Salesforce Baseline Standard. You can upload up to five custom baselines to use instead of the Salesforce Baseline Standard.

Auditing

Auditing provides information about use of the system, which can be critical in diagnosing potential or real security issues. The Salesforce auditing features don't secure your organization by themselves; someone in your organization should do regular audits to detect potential abuse.

Salesforce Shield

Salesforce Shield is a trio of security tools that admins and developers can use to build a new level of trust, transparency, compliance, and governance right into business-critical apps. It includes Platform Encryption, Event Monitoring, and Field Audit Trail. Ask your Salesforce administrator if Salesforce Shield is available in your organization.

SEE ALSO:

Security Implementation Guide

Phishing and Malware

Trust starts with transparency. That's why Salesforce displays real-time information on system performance and security on the trust site at http://trust.salesforce.com. This site provides live data on system performance, alerts for current and recent phishing and malware attempts, and tips on best security practices for your organization.

The Security tab on the trust site includes valuable information that can help you to safeguard your company's data. In particular, be on the alert for phishing and malware.

- Phishing is a social engineering technique that attempts to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishers often direct users to enter details at a fake website whose URL and look-and-feel are almost identical to the legitimate one. As the Salesforce community grows, it has become an increasingly appealing target for phishers. You will never get an email or a phone call from a Salesforce employee asking you to reveal a password, so don't reveal it to anyone. You can report any suspicious activities by clicking the **Report a Suspicious Email** link under the **Trust** tab at http://trust.salesforce.com.
- Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. It is a general term used to cover a variety of forms of hostile, intrusive, or annoying software, and it includes computer viruses and spyware.

What Salesforce Is Doing About Phishing and Malware

Customer security is the foundation of customer success, so Salesforce continues to implement the best possible practices and technologies in this area. Recent and ongoing actions include:

- Actively monitoring and analyzing logs to enable proactive alerts to customers who have been affected.
- Collaborating with leading security vendors and experts on specific threats.
- Executing swift strategies to remove or disable fraudulent sites (often within an hour of detection).
- Reinforcing security education and tightening access policies within Salesforce.
- Evaluating and developing new technologies both for our customers and for deployment within our infrastructure.

What Salesforce Recommends You Do

Salesforce is committed to setting the standards in software-as-a-service as an effective partner in customer security. So, in addition to internal efforts, Salesforce strongly recommends that customers implement the following changes to enhance security:

- Modify your Salesforce implementation to activate IP range restrictions. This allows users to access Salesforce only from your corporate network or VPN. For more information, see Restrict Where and When Users Can Log In to Salesforce on page 574.
- Set session security restrictions to make spoofing more difficult. For more information, see Modify Session Security Settings on page 585.
- Educate your employees not to open suspect emails and to be vigilant in guarding against phishing attempts.
- Use security solutions from leading vendors to deploy spam filtering and malware protection.
- Designate a security contact within your organization so that Salesforce can more effectively communicate with you. Contact your Salesforce representative with this information.
- Consider using two-factor authentication techniques to restrict access to your network. For more information, see Two-Factor Authentication on page 568.
- Use Transaction Security to monitor events and take appropriate actions. For more information, see Transaction Security Policies on page 613.

Salesforce has a Security Incident Response Team to respond to any security issues. To report a security incident or vulnerability to Salesforce, contact security@salesforce.com. Describe the issue in detail, and the team will respond promptly.

Security Infrastructure

Salesforce utilizes some of the most advanced technology for Internet security available today. When you access the application using a Salesforce-supported browser, Transport Layer Security (TLS) technology protects your information using both server authentication and Classic Encryption, ensuring that your data is safe, secure, and available only to registered users in your organization.

One of the core features of a multi-tenant platform is the use of a single pool of computing resources to service the needs of many different customers. Salesforce protects your organization's data from all other customer organizations by using a unique organization identifier, which is associated with each user's session. Once you log in to your organization, your subsequent requests are associated with your organization, using this identifier.

In addition, Salesforce is hosted in a secure server environment that uses a firewall and other advanced technology to prevent interference or access from outside intruders.

Security Health Check

As an admin, you can use Health Check to identify and fix potential vulnerabilities in your security settings, all from a single page. A summary score shows how your org measures against a security baseline, like the Salesforce Baseline Standard. You can upload up to five custom baselines to use instead of the Salesforce Baseline Standard.

From Setup, enter `Health Check` in the **Quick Find** box, then select **Health Check**.

In the baseline dropdown (1), choose the Salesforce Baseline Standard or a custom baseline. The baseline consists of recommended values for High-Risk, Medium-Risk, Low-Risk, and Informational Security Settings (2). If you change settings to be less restrictive than what's in the baseline, your health check score decreases.

Your settings are shown with information about how they compare against baseline values (3). To remediate a risk, edit the setting (4) or use Fix Risks (5) to quickly change settings to your selected baseline's recommended values without leaving the Health Check page. You can import, export, edit, or delete a custom baseline (6).

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

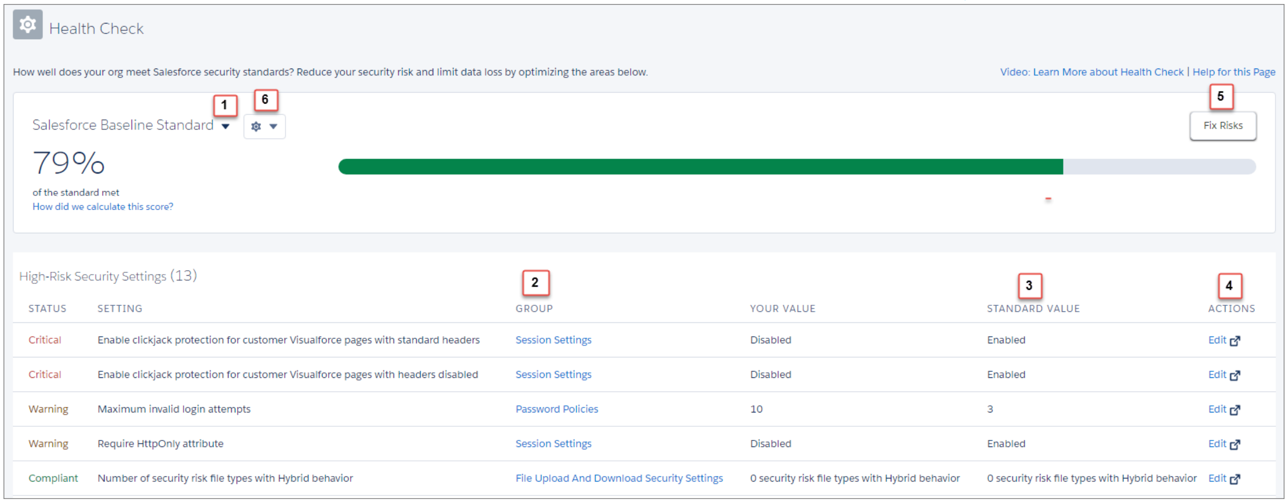
USER PERMISSIONS

To view Health Check and export custom baselines:

- View Health Check

To import custom baselines:

- Manage Health Check



How well does your org meet Salesforce security standards? Reduce your security risk and limit data loss by optimizing the areas below.

Video: Learn More about Health Check | Help for this Page

Salesforce Baseline Standard

79%

of the standard met

How did we calculate this score?

High-Risk Security Settings (13)

STATUS	SETTING	GROUP	YOUR VALUE	STANDARD VALUE	ACTIONS
Critical	Enable clickjack protection for customer Visualforce pages with standard headers	Session Settings	Disabled	Enabled	Edit
Critical	Enable clickjack protection for customer Visualforce pages with headers disabled	Session Settings	Disabled	Enabled	Edit
Warning	Maximum invalid login attempts	Password Policies	10	3	Edit
Warning	Require HttpOnly attribute	Session Settings	Disabled	Enabled	Edit
Compliant	Number of security risk file types with Hybrid behavior	File Upload And Download Security Settings	0 security risk file types with Hybrid behavior	0 security risk file types with Hybrid behavior	Edit

Example: Suppose that you changed your password minimum length from 8 (the default value) to 5, and changed other Password Policies settings to be less restrictive. These changes make your users' passwords more vulnerable to guessing and other brute force attacks. As a result, your overall score decreases, and the settings are listed as risks.

Fix Risks Limitations

Not all settings can be changed using the Fix Risks button. If a setting you want to adjust does not appear on the Fix Risks screen, change them manually using the Edit link on the Health Check page.

IN THIS SECTION:

How Is the Health Check Score Calculated?

The Health Check score is calculated by a proprietary formula that measures how well your security settings meet either the Salesforce Baseline Standard or your selected custom baseline. Settings that meet or exceed compliance raise your score, and settings at risk lower your score.

Create a Custom Baseline for Health Check

You can import up to five custom baselines to compare your org's security settings with your own standards, instead of using Salesforce recommended standards. For example, if you're a financial industry business, you can create a custom security baseline using FINRA standards.

Custom Baseline File Requirements

To import your Health Check custom baseline successfully, make sure that your file and settings meet the requirements.

SEE ALSO:

How Is the Health Check Score Calculated?

Security Implementation Guide

How Is the Health Check Score Calculated?

The Health Check score is calculated by a proprietary formula that measures how well your security settings meet either the Salesforce Baseline Standard or your selected custom baseline. Settings that meet or exceed compliance raise your score, and settings at risk lower your score.

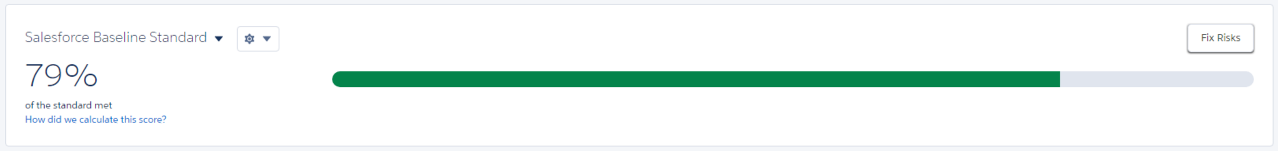
There are four risk categories: High-Risk, Medium-Risk, Low-Risk, and Informational. The risk categories affect your Health Check score, with High-Risk settings counting the most, Low-Risk settings counting the least, and Medium-Risk settings, well, they're in the middle. Settings in the Informational category do not factor into your Health Check score. For details, see Salesforce Baseline Standard on page 497.

If all settings meet or exceed the standard, your total score is 100%. As you update your settings, your green bar moves to the right!

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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


Salesforce Baseline Standard ▾
⚙ ▾
Fix Risks
79%
of the standard met
How did we calculate this score?

Recommended Actions Based on Your Score

If your total score is...	We recommend to...
0–33%	Remediate high risks immediately
34–66%	Remediate high risks in the short term, and medium risks in the long term
67–100%	Review Health Check periodically to remediate risks

Note: New Salesforce orgs have an initial score less than 100%. Use Health Check to quickly improve your score by eliminating high risks in your Password Policies and other setting groups.

The Salesforce Baseline Standard

The following are the settings, risk levels, and values from the default Salesforce Baseline Standard. If you are using a custom baseline, your information differs.

High Risk Security Settings

Setting	Compliant Value	Warning Value	Critical Value
Lock sessions to the domain in which they were first used	Checkbox selected	N/A	Checkbox deselected
Enable the SMS method of identity confirmation	Checkbox selected	N/A	Checkbox deselected
Enable clickjack protection for Setup pages	Checkbox selected	N/A	Checkbox deselected
Enable clickjack protection for non-Setup for Salesforce pages	Checkbox selected	N/A	Checkbox deselected
Enable clickjack protection for customer VisualForce pages with standard headers	Checkbox selected	N/A	Checkbox deselected
Enable clickjack protection for customer VisualForce pages with headers disabled	Checkbox selected	N/A	Checkbox deselected
Enable CSRF protection on GET requests on non-setup pages	Checkbox selected	N/A	Checkbox deselected
Enable CSRF protection on POST requests on non-setup pages	Checkbox selected	N/A	Checkbox deselected
Require Secure Connections (HTTPS)	Checkbox selected	N/A	Checkbox deselected
Require HttpOnly attribute	Checkbox selected	Checkbox deselected	N/A
File Upload And Download Security Settings	No security risk file types have hybrid behavior enabled.	One or more security risk file types has hybrid behavior enabled.	N/A
Maximum invalid login attempts	3	5, 10	No Limit

Medium Risk Security Settings

Setting	Compliant Value	Warning Value	Critical Value
Require a minimum 1 day password lifetime	Checkbox selected	Checkbox deselected	N/A
Force relogin after Login-As-User	Checkbox selected	N/A	Checkbox deselected
Enforce login IP ranges on every request	Checkbox selected	Checkbox deselected	N/A
Administrators Can Log In As Any User	Checkbox deselected	Checkbox selected	N/A

Setting	Compliant Value	Warning Value	Critical Value
Enforce password history	3 or more passwords remembered	1 or 2 passwords remembered	No passwords remembered
Minimum password length	8	6 or 7	5 or less
User passwords expire in	90 days or less	180 days	One year or Never expires
Password complexity requirement	Must mix alpha, numeric, and special characters, or more complex	Must mix alpha and numeric characters	No restriction

Low Risk Security Settings

Setting	Compliant Value	Warning Value	Critical Value
Obscure secret answer for password resets	Checkbox selected	Checkbox deselected	N/A
Force logout on session timeout	Checkbox selected	Checkbox deselected	N/A
Remote Site	No remote sites with the Disable Protocol Security option selected	At least one remote site created with the **Disable Protocol Security** option selected.	N/A
Expiration Date	No certificates created, or all certificates have more than 180 days until expiration	Less than 180 days but more than 15 days until expiration of at least one certificate	Less than 15 days until expiration of at least one certificate
Password question requirement	Cannot contain password	None	N/A
Timeout Value	2 hours or less	4, 8, or 12 hours	Checkbox deselected
Lockout effective period	30 minutes or greater	Less than 30 minutes	N/A

Informational Security Settings

Informational Security settings do not affect your Health Check score, but are valuable to review.

Setting	Compliant Value	Warning Value	Critical Value
Key Size	All certificates have a key size of 4096	At least one certificate has a key size of 2048	N/A

SEE ALSO:

Security Health Check

Create a Custom Baseline for Health Check

EDITIONS

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

USER PERMISSIONS

To view a custom baseline

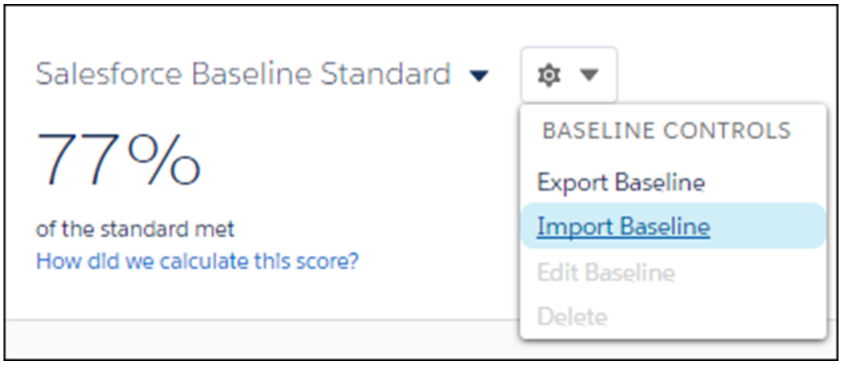
- View Health Check

To create a custom baseline

- Manage Health Check

You can import up to five custom baselines to compare your org's security settings with your own standards, instead of using Salesforce recommended standards. For example, if you're a financial industry business, you can create a custom security baseline using FINRA standards.

To create a custom baseline, start with the Salesforce Baseline Standard.



1. Export the Salesforce Baseline Standard file by selecting **Export Baseline** from the Baseline Controls menu.
2. Edit the XML file with a text editor.
   a. Adjust the risk categories to customize your scoring. The risk category affects your Health Check score. A setting in a higher risk category is weighted as more important than a lower one. Moving a setting to the Informational category removes it from the Health Check score calculation.
   b. Modify the setting values by following the Custom Baseline File Requirements. You can't change some values, and some settings have restricted value options. Do not add or delete risk categories, setting names, or quotation marks. If you do, your import fails.

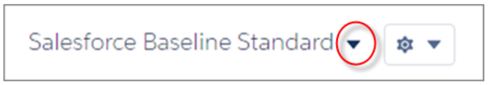
      Note: In some security settings, a low value could be low risk, but in others, it could be high risk. For example, the lower your minimum password length value is, the riskier it is. But the lower your maximum invalid login attempts value is, the safer it is.

3. Save your file, and import it by choosing **Import Baseline** from the Baseline Controls menu. A dialog box opens.
   a. Name your custom baseline. Spaces and some special characters are allowed. If the name is "SFDC recommended" or "Salesforce Baseline Standard," your file fails to import.
   b. Give your custom baseline an API name. The API name must be unique. You can use letters and numbers, but the name must begin with a letter. It cannot contain spaces or special characters.
   c. Make your custom baseline the default baseline in Security Health Check, if you choose.

Note:

- Unexpected information in the baseline file causes the import to fail. If your import fails, you receive a message to help resolve the problem. See Custom Baseline File Requirements in Salesforce Help for troubleshooting assistance.
- You can change the baseline name, API name, and default baseline using the Edit feature in the Baseline Controls menu.

4. To confirm that your file uploaded, click the baseline dropdown and select your baseline. If you set your custom baseline as the default, it will be displayed after import.



SEE ALSO:

Custom Baseline File Requirements

How Is the Health Check Score Calculated?

Security Health Check

Custom Baseline File Requirements

To import your Health Check custom baseline successfully, make sure that your file and settings meet the requirements.

EDITIONS

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

XML File

Use a valid XML file with only English language characters. The file cannot be larger than 20 KB. Make sure that each value is surrounded in quotation marks. Be careful not to delete any of them when editing the file.

Custom Baseline Security Setting Fields and Values

You cannot add or delete the Health Check settings from the file, but you can change their risks and values.

There are four risk categories: High-Risk, Medium-Risk, Low-Risk, and Informational. The risk categories affect your Health Check score, with High-Risk settings counting the most, Low-Risk settings counting the least, and Medium-Risk settings, well, they're in the middle. You can move settings into any risk category. Settings in the Informational category do not factor into your Health Check score, so move settings that are unnecessary to your org to this category rather than deleting them.

Each security setting shows in Health Check as either compliant, warning, or critical. These statuses guide you to make your org more secure. Assign values to each status in the import file.

There are three setting types: boolean, numeric range, and enum. The values you can assign to each setting depend on the setting type.

Boolean Security Settings

Boolean settings have two attributes—compliant and noncompliant. Compliant values correspond to checkboxes in security settings. A Boolean value of `"true"` indicates selecting the checkbox, and `"false"` represents deselecting it. Noncompliant attributes can take either `warning` or `critical` values.

Important: You cannot change boolean compliant values in Health Check, although you can change noncompliant values.

Setting	Accepted Values
LoginAccessPolicies.adminLoginAsAnyUser	• “false”—compliant • “warning” or “critical”—noncompliant
SessionSettings.clickjackSetup	• “true”—compliant • “warning” or “critical”—noncompliant
SessionSettings.clickjackNonSetup	• “true”—compliant • “warning” or “critical”—noncompliant
SessionSettings.clickjackVisualForceHeaders	• “true”—compliant • “warning” or “critical”—noncompliant
SessionSettings.clickjackVisualForceNoHeaders	• “true”—compliant • “warning” or “critical”—noncompliant
SessionSettings.csrfGet	• “true”—compliant • “warning” or “critical”—noncompliant
SessionSettings.csrfPost	• “true”—compliant • “warning” or “critical”—noncompliant
SessionSettings.enableSmsIdentity	• “true”—compliant • “warning” or “critical”—noncompliant
SessionSettings.enforceLoginIp	• “true”—compliant • “warning” or “critical”— noncompliant
SessionSettings.forceLogoutOnTimeout	• “true”—compliant • “warning” or “critical”—noncompliant
SessionSettings.forceRelogin	• “true”—compliant • “warning” or “critical”—noncompliant
SessionSettings.lockSessionsToDomain	• “true”—compliant • “warning” or “critical”—noncompliant

Setting	Accepted Values
SessionSettings.requireSecureConnections	• “true”—compliant • “warning” or “critical”—noncompliant
SessionSettings.requireHttpOnly	• “true”— compliant • “warning” or “critical”— noncompliant
PasswordPolicies.minOneDayPasswordLifetime	• “true”— compliant • “warning” or “critical”— noncompliant
PasswordPolicies.obscureSecretAnswer	• “true”—compliant • “warning” or “critical”—noncompliant

Numeric Range Security Settings

Numeric range values are positive integers extended to one decimal place. You provide compliant and warning values only for numeric range settings. Critical values are assumed based on the other values in the settings. Each setting has specific validation rules, so enter only acceptable values.

Setting	Compliant Value	Warning Value
PasswordPolicies.history	Any integer between “0.0” and “24.0”	Any integer between “0.0” and “24.0” that is less than the compliant value Note: Any value less than the warning value shows as critical
CertificateAndKeyManagement.certExpiration	Number of days—Any integer between “0.0” and “180.0”	Any integer between “0.0” and “180.0” that is less than the compliant value Note: Any value less than the warning value shows as critical
FileUploadAndDownloadSecurity.hybridSecurityRiskFileTypes	Any integer “0.0” or greater	Any integer greater than the compliant value Note: Any value greater than the warning value shows as critical
CertificateAndKeyManagement.keySize	“4096.0” or “2048.0”	“4096.0” or “2048.0” Note: To not allow the 2048 key size, enter a compliant value of “4096.0” and a warning value of any number between “2048.0” and “4096.0”.

Setting	Compliant Value	Warning Value
PasswordPolicies.minPasswordLength	Any integer between “5.0” and “50.0”	Any integer between “5.0” and “50.0” that is less than the compliant value Note: Any value less than the warning value shows as critical
RemoteSiteSettings.remoteSiteSettings	Maximum number of remote site settings allowed—Any integer greater than “0.0”	Any integer greater than the compliant value Note: Any value greater than the warning value shows as critical

Enum Security Settings

Enum values allow you to choose between provided string texts. Use all the possible values, and decide whether they are compliant, warning, or critical status. Enum values are case-sensitive. You can assign multiple enum names to one status by separating them with commas, for example, compliant="FifteenMinutes,ThirtyMinutes,SixtyMinutes,TwoHours".

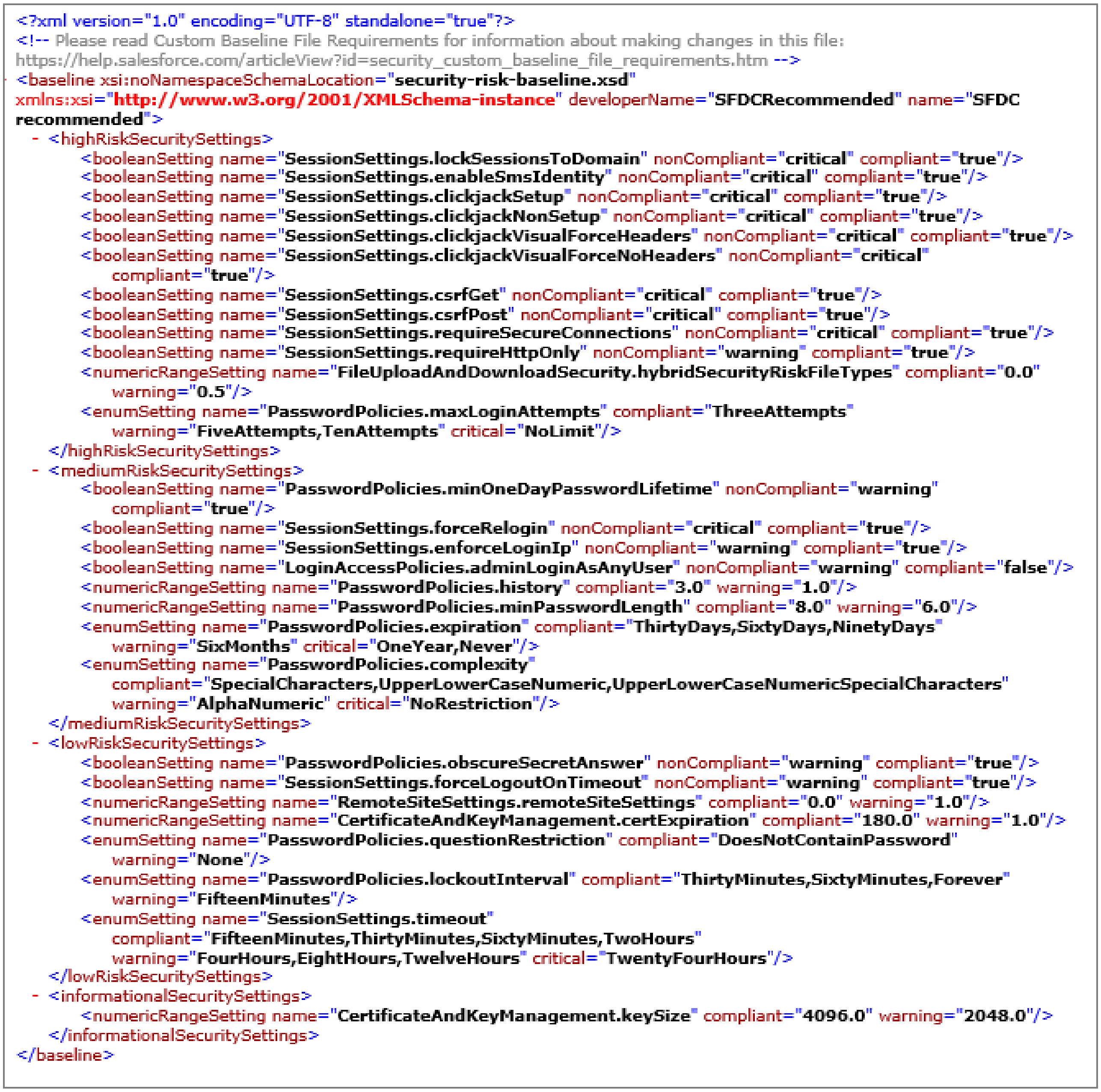
As long as all values are used, you can leave a status empty. For example, you could have all the values split between compliant and critical and leave warning empty: `warning=“”`. Do not leave the compliant status empty.

Important: Use every accepted value in each setting. If a value is missing, the file doesn’t import.

Setting	Accepted Values
PasswordPolicies.complexity	• “UpperLowerCaseNumericSpecialCharacters” • “UpperLowerCaseNumeric” • “SpecialCharacters” • “AlphaNumeric” • “NoRestriction” (highest risk)
PasswordPolicies.expiration	• “ThirtyDays” • “SixtyDays” • “NinetyDays” • “SixMonths” • “OneYear” • “Never” (highest risk)
PasswordPolicies.lockoutInterval	• “Forever” (admin must reset) • “SixtyMinutes” • “ThirtyMinutes” • “FifteenMinutes” (highest risk)
PasswordPolicies.maxLoginAttempts	• “ThreeAttempts”

Setting	Accepted Values
	• "FiveAttempts" • "TenAttempts" • "NoLimit" (highest risk)
PasswordPolicies.questionRestriction	• "DoesNotContainPassword" • "None" (highest risk)
SessionSettings.timeout	• "FifteenMinutes" • "ThirtyMinutes" • "SixtyMinutes" • "TwoHours" • "FourHours" • "EightHours" • "TwelveHours" • "TwentyFourHours" (highest risk)

Example:



```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<!-- Please read Custom Baseline File Requirements for information about making changes in this file:
https://help.salesforce.com/articleView?id=security_custom_baseline_file_requirements.htm -->
<baseline xsi:noNamespaceSchemaLocation="security-risk-baseline.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" developerName="SFDCRecommended" name="SFDC
recommended">
 - <highRiskSecuritySettings>
       <booleanSetting name="SessionSettings.lockSessionsToDomain" nonCompliant="critical" compliant="true"/>
       <booleanSetting name="SessionSettings.enableSmsIdentity" nonCompliant="critical" compliant="true"/>
       <booleanSetting name="SessionSettings.clickjackSetup" nonCompliant="critical" compliant="true"/>
       <booleanSetting name="SessionSettings.clickjackNonSetup" nonCompliant="critical" compliant="true"/>
       <booleanSetting name="SessionSettings.clickjackVisualForceHeaders" nonCompliant="critical" compliant="true"/>
       <booleanSetting name="SessionSettings.clickjackVisualForceNoHeaders" nonCompliant="critical"
          compliant="true"/>
       <booleanSetting name="SessionSettings.csrfGet" nonCompliant="critical" compliant="true"/>
       <booleanSetting name="SessionSettings.csrfPost" nonCompliant="critical" compliant="true"/>
       <booleanSetting name="SessionSettings.requireSecureConnections" nonCompliant="critical" compliant="true"/>
       <booleanSetting name="SessionSettings.requireHttpOnly" nonCompliant="warning" compliant="true"/>
       <numericRangeSetting name="FileUploadAndDownloadSecurity.hybridSecurityRiskFileTypes" compliant="0.0"
          warning="0.5"/>
       <enumSetting name="PasswordPolicies.maxLoginAttempts" compliant="ThreeAttempts"
          warning="FiveAttempts,TenAttempts" critical="NoLimit"/>
   </highRiskSecuritySettings>
 - <mediumRiskSecuritySettings>
       <booleanSetting name="PasswordPolicies.minOneDayPasswordLifetime" nonCompliant="warning"
          compliant="true"/>
       <booleanSetting name="SessionSettings.forceRelogin" nonCompliant="critical" compliant="true"/>
       <booleanSetting name="SessionSettings.enforceLoginIp" nonCompliant="warning" compliant="true"/>
       <booleanSetting name="LoginAccessPolicies.adminLoginAsAnyUser" nonCompliant="warning" compliant="false"/>
       <numericRangeSetting name="PasswordPolicies.history" compliant="3.0" warning="1.0"/>
       <numericRangeSetting name="PasswordPolicies.minPasswordLength" compliant="8.0" warning="6.0"/>
       <enumSetting name="PasswordPolicies.expiration" compliant="ThirtyDays,SixtyDays,NinetyDays"
          warning="SixMonths" critical="OneYear,Never"/>
       <enumSetting name="PasswordPolicies.complexity"
          compliant="SpecialCharacters,UpperLowerCaseNumeric,UpperLowerCaseNumericSpecialCharacters"
          warning="AlphaNumeric" critical="NoRestriction"/>
   </mediumRiskSecuritySettings>
 - <lowRiskSecuritySettings>
       <booleanSetting name="PasswordPolicies.obscureSecretAnswer" nonCompliant="warning" compliant="true"/>
       <booleanSetting name="SessionSettings.forceLogoutOnTimeout" nonCompliant="warning" compliant="true"/>
       <numericRangeSetting name="RemoteSiteSettings.remoteSiteSettings" compliant="0.0" warning="1.0"/>
       <numericRangeSetting name="CertificateAndKeyManagement.certExpiration" compliant="180.0" warning="1.0"/>
       <enumSetting name="PasswordPolicies.questionRestriction" compliant="DoesNotContainPassword"
          warning="None"/>
       <enumSetting name="PasswordPolicies.lockoutInterval" compliant="ThirtyMinutes,SixtyMinutes,Forever"
          warning="FifteenMinutes"/>
       <enumSetting name="SessionSettings.timeout"
          compliant="FifteenMinutes,ThirtyMinutes,SixtyMinutes,TwoHours"
          warning="FourHours,EightHours,TwelveHours" critical="TwentyFourHours"/>
   </lowRiskSecuritySettings>
 - <informationalSecuritySettings>
       <numericRangeSetting name="CertificateAndKeyManagement.keySize" compliant="4096.0" warning="2048.0"/>
   </informationalSecuritySettings>
</baseline>
```

SEE ALSO:

Create a Custom Baseline for Health Check

Auditing

Auditing provides information about use of the system, which can be critical in diagnosing potential or real security issues. The Salesforce auditing features don't secure your organization by themselves; someone in your organization should do regular audits to detect potential abuse.

To verify that your system is actually secure, you should perform audits to monitor for unexpected changes or usage trends.

Record Modification Fields

All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.

Login History

You can review a list of successful and failed login attempts to your organization for the past six months. See Monitor Login History on page 777.

Field History Tracking

You can also enable auditing for individual fields, which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing. See Field History Tracking on page 788.

Setup Audit Trail

Administrators can also view a Setup Audit Trail, which logs when modifications are made to your organization's configuration. See Monitor Setup Changes on page 785.

Salesforce Shield

Salesforce Shield is a trio of security tools that admins and developers can use to build a new level of trust, transparency, compliance, and governance right into business-critical apps. It includes Platform Encryption, Event Monitoring, and Field Audit Trail. Ask your Salesforce administrator if Salesforce Shield is available in your organization.

Platform Encryption

Platform Encryption allows you to natively encrypt your most sensitive data at rest across all your Salesforce apps. This helps you protect PII, sensitive, confidential, or proprietary data and meet both external and internal data compliance policies while keeping critical app functionality — like search, workflow, and validation rules. You keep full control over encryption keys and can set encrypted data permissions to protect sensitive data from unauthorized users. See Platform Encryption. on page 507

Event Monitoring

Event Monitoring gives you access to detailed performance, security, and usage data on all your Salesforce apps. Every interaction is tracked and accessible via API, so you can view it in the data visualization app of your choice. See who is accessing critical business data when, and from where. Understand user adoption across your apps. Troubleshoot and optimize performance to improve end-user experience. Event Monitoring data can be easily imported into any data visualization or application monitoring tool like Wave Analytics, Splunk, or New Relic. To get started, check out our Event Monitoring training course.

Field Audit Trail

Field Audit Trail lets you know the state and value of your data for any date, at any time. You can use it for regulatory compliance, internal governance, audit, or customer service. Built on a big data backend for massive scalability, Field Audit Trail helps companies create a forensic data-level audit trail with up to 10 years of history, and set triggers for when data is deleted. See Field Audit Trail on page 792.

Strengthen Your Data's Security with Shield Platform Encryption

Shield Platform Encryption gives your data a whole new layer of security while preserving critical platform functionality. It enables you to encrypt sensitive data at rest, and not just when transmitted over a network, so your company can confidently comply with privacy policies, regulatory requirements, and contractual obligations for handling private data.

Shield Platform Encryption builds on the data encryption options that Salesforce offers out of the box. Data stored in many standard and custom fields and in files and attachments is encrypted using an advanced HSM-based key derivation system, so it is protected even when other lines of defense have been compromised.

Your data encryption key is never saved or shared across organizations. Instead, it is derived on demand from a master secret and your organization-specific tenant secret, and cached on an application server.

You can try out Shield Platform Encryption at no charge in Developer Edition orgs. It is available in sandboxes after it has been provisioned for your production org.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

IN THIS SECTION:

Encrypt Fields and Files

Specify the fields and files you want to encrypt. Remember that encryption is not the same thing as field-level security or object-level security. Those should already be in place before you implement your encryption strategy.

Manage Shield Platform Encryption

To provide Shield Platform Encryption for your organization, contact your Salesforce account executive. They'll help you provision the correct license so you can get started on creating your own unique tenant secret.

How Shield Platform Encryption Works

Shield Platform Encryption relies on a unique tenant secret that you control and a master secret that's maintained by Salesforce. We combine these secrets to create your unique data encryption key. We use that key to encrypt data that your users put into Salesforce, and to decrypt data when your authorized users need it.

Platform Encryption Best Practices

Take the time to identify the most likely threats to your organization. This will help you distinguish data that needs encryption from data that doesn't, so that you can encrypt only what you need to. Make sure that your tenant secret and keys are backed up, and be careful who you allow to manage your secrets and keys.

Tradeoffs and Limitations of Shield Platform Encryption

A security solution as powerful as Shield Platform Encryption doesn't come without some tradeoffs. When your data is encrypted, some users may see limitations to some functionality, and a few features aren't available at all. Consider the impact on your users and your overall business solution as you design your encryption strategy.

SEE ALSO:

Salesforce Platform Encryption Implementation Guide

What's the Difference Between Classic Encryption and Shield Platform Encryption?

Salesforce Platform Encryption Architecture

Encrypt Fields and Files

Specify the fields and files you want to encrypt. Remember that encryption is not the same thing as field-level security or object-level security. Those should already be in place before you implement your encryption strategy.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

IN THIS SECTION:

Encrypt New Data in Fields

Select the fields you want to encrypt. For best results, encrypt the smallest possible number of fields.

Encrypt New Files and Attachments

For another layer of data protection, encrypt files and attachments. If Shield Platform Encryption is on, the body of each file or attachment is encrypted when it's uploaded.

Keep Your Data Encryption Up To Date

To get the most protection out of your encryption strategy, it's important to keep your encryption status up to date. Salesforce Support is here to help you synchronize your data with your most recent encryption key management policies and configuration.

Fix Compatibility Problems

When you select fields or files to encrypt, Salesforce automatically checks for potential side effects and warns you if any existing settings may pose a risk to data access or your normal use of Salesforce. You have some options for how to clear up these problems.

Use Encrypted Data in Formulas

Use custom formula fields to quickly find encrypted data. You can write formulas with several operators and functions, render encrypted data in text, date, and date/time formats, and reference quick actions.

Encrypt Data in Chatter

Enabling Shield Platform Encryption for Chatter adds an extra layer of security to information that users share in Chatter. You can encrypt data at rest in feed posts and comments, questions and answers, link names and URLs, poll questions and choices, and content from your custom rich publisher apps.

SEE ALSO:

Platform Encryption Overview

Encrypt New Data in Fields

Select the fields you want to encrypt. For best results, encrypt the smallest possible number of fields.

Depending on the size of your organization, enabling a standard field for encryption can take a few minutes.

1. Make sure that your organization has an active encryption key. If you're not sure, check with your administrator.
2. From Setup, use the `Quick Find` box to find the Platform Encryption setup page.
3. Click **Encrypt Fields**.
4. Click **Edit**.
5. Select the fields you want to encrypt, and save your settings.

The automatic Platform Encryption validation service checks for settings in your organization that can block encryption. You'll receive an email with suggestions for fixing any incompatible settings.

Field values are automatically encrypted only in records created or updated after you've enabled encryption. Contact Salesforce to update existing records so that their field values are encrypted.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

SEE ALSO:

- Which Standard Fields Can I Encrypt?
- Which Custom Fields Can I Encrypt?
- Field Limits with Shield Platform Encryption
- Data Loader
- Why Isn't My Encrypted Data Masked?
- API Guide: CustomField
- Use Encrypted Data in Formulas

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:

- View Setup and Configuration

To encrypt fields:

- Customize Application

Encrypt New Files and Attachments

For another layer of data protection, encrypt files and attachments. If Shield Platform Encryption is on, the body of each file or attachment is encrypted when it's uploaded.

Note: Before you begin, make sure that your organization has an active encryption key; if you're not sure, check with your administrator.

1. From Setup, enter `Platform Encryption` in the `Quick Find` box, then select **Platform Encryption**.
2. Select **Encrypt Files and Attachments**.
3. Click **Save**.

Important: Users with access to the file can work normally with it regardless of their encryption-specific permissions. Users who are logged in to your org and have read access can search and view the body content.

Users can continue to upload files and attachments per the usual file size limits. Expansion of file sizes caused by encryption doesn't count against these limits.

Turning on file and attachment encryption affects new files and attachments. It doesn't automatically encrypt files and attachments that were already in Salesforce. To encrypt existing files, contact Salesforce.

To check whether a file or attachment is encrypted, look for the encryption indicator on the detail page of the file or attachment. You can also query the `isEncrypted` field on the ContentVersion object (for files) or on the Attachment object (for attachments).

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

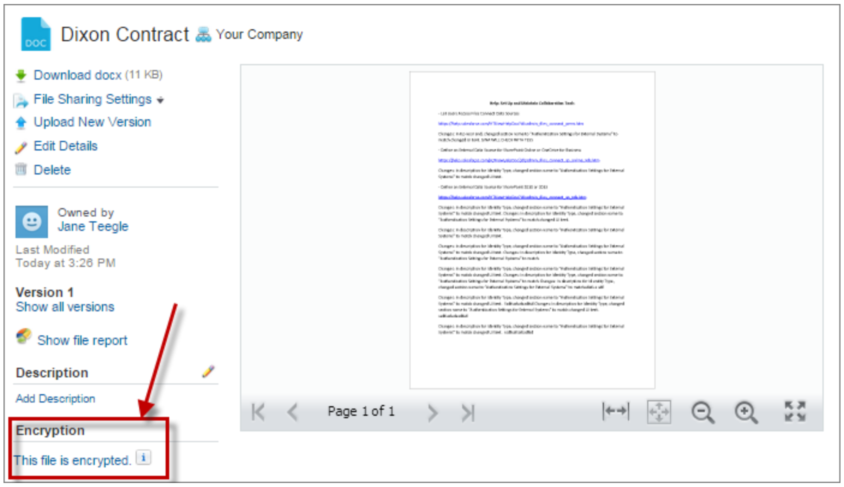
Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:
- View Setup and Configuration

To encrypt files:
- Customize Application

Here's What It Looks Like When a File Is Encrypted.



Dixon Contract Your Company

Owned by Jane Teegle

Last Modified Today at 3:26 PM

Version 1

Encryption

This file is encrypted.

SEE ALSO:

- Which Files Are Encrypted?
- Data Loader
- The ContentVersion object
- API Guide: Attachment

Keep Your Data Encryption Up To Date

To get the most protection out of your encryption strategy, it's important to keep your encryption status up to date. Salesforce Support is here to help you synchronize your data with your most recent encryption key management policies and configuration.

- When you turn on encryption, data that was already there doesn't automatically get encrypted. Our background encryption service takes care of that on request.
- When you change your tenant secret as part of your key rotation strategy, data that's already encrypted remains encrypted with the old tenant secret. Our background encryption service can update it on request. And don't worry, you always have access to your data as long as you don't destroy the old, archived keys.
- If you turn off encryption, data that's already there remains encrypted, and the tradeoffs and limitations that apply to encrypted data are still in place. Our background encryption service will decrypt the data for you, restoring any missing functionality, on request.

Note: Syncing your data encryption does not affect the record timestamp. It doesn't execute triggers, validation rules, workflow rules, or any other automated service.

How to Request a Background Encryption Update

Allow lead time

Contact Salesforce support at least a week before you need the background encryption completed.

Specify the fields

Provide the list of fields you want encrypted, re-encrypted, or decrypted.

Verify the list

Verify that this list matches the set of standard fields you have marked for encryption on the Encryption Setup page, and the custom fields you have marked on the Field Definition page.

Tip: Also check that your field values aren't too long for encryption.

Include files and attachments?

Verify that your specified fields match those marked for encryption on the Encryption Setup and Field Definition pages. (Encryption for files and attachments is all or nothing. You don't have to specify which ones.)

Include history and feed data?

Specify whether you want the corresponding Field History and feed data encrypted.

Choose a time

Select your preferred off-peak maintenance window. We will try to accommodate your needs.

Special Situations

It's rare, but not impossible, that your encryption key has been destroyed. If this is the case, and you want to re-encrypt your data, you have some options.

- Re-import the destroyed key from a backup, then ask Salesforce support to synchronize your data with your encryption policy.
- Delete all the data that was encrypted with the destroyed key, then ask Salesforce support to synchronize your data.
- Ask Salesforce support to overwrite all the data that was encrypted with the destroyed key, using characters such as "?????", and synchronize your data.

If Salesforce support re-encrypts your data with a new key, any data that was encrypted with the destroyed key is skipped.

When you disable encryption for files that were encrypted with a key that's been destroyed, the files don't automatically go away. You can ask Salesforce support to delete the files.

Tip: If you're not sure which data is already encrypted, you can refresh your memory by visiting the Encryption Statistics page, which keeps a record of all the fields that you have encrypted. To see that page in your Setup menu, ask Salesforce support to enable the Encryption Statistics beta for your org.

SEE ALSO:

General Shield Platform Encryption Considerations

Field Limits with Shield Platform Encryption

Fix Compatibility Problems

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

When you select fields or files to encrypt, Salesforce automatically checks for potential side effects and warns you if any existing settings may pose a risk to data access or your normal use of Salesforce. You have some options for how to clear up these problems.

If your results include error messages, you're probably running into one or more of these limitations:

Portals

You can't encrypt standard fields, because a customer portal or a partner portal is enabled in your organization. To deactivate a customer portal, go to the Customer Portal Settings page in Setup. To deactivate a partner portal, go to the Partners page in Setup.

Note: Communities are not related to this issue. They are fully compatible with encryption.

Criteria-Based Sharing Rules

You've selected a field that is used in a filter in a criteria-based sharing rule.

SOQL/SOSL queries

You've selected a field that's used in an aggregate function in a SOQL query, or in a WHERE, GROUP BY, or ORDER BY clause.

Formula fields

You've selected a field that's referenced by a custom formula field in an unsupported way. Formulas can use BLANKVALUE, CASE, HYPERLINK, IF, IMAGE, ISBLANK, ISNULL, and NULLVALUE, as well as concatenation (&).

Flows and Processes

You've selected a field that's used in one of these contexts.

- To filter data in a flow
- To sort data in a flow
- To filter data in a process
- To filter data in a dynamic record choice
- To sort data in a dynamic record choice

Note: By default, your results only list the first 250 errors per element. You can increase the number of errors listed in your results to 5000. Contact Salesforce for help.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

SEE ALSO:

Back to Parent Topic

Use Encrypted Data in Formulas

Use custom formula fields to quickly find encrypted data. You can write formulas with several operators and functions, render encrypted data in text, date, and date/time formats, and reference quick actions.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Supported Operators, Functions, and Actions

Supported operators and functions:

- `&` and `+` (concatenate)
- `BLANKVALUE`
- `CASE`
- `HYPERLINK`
- `IF`
- `IMAGE`
- `ISBLANK`
- `ISNULL`
- `NULLVALUE`

Also supported:

- Spanning
- Quick actions

Formulas can return data only in `text`, `date`, or `date/time` formats.

`&` And `+` (Concatenate)

This works:	`(encryptedField__c & encryptedField__c)`
Why it works:	This works because `&` is supported.
This doesn't work:	`LOWER(encryptedField__c & encryptedField__c)`
Why it doesn't work:	`LOWER` isn't a supported function, and the input is an encrypted value.

Case

`CASE` returns encrypted field values, but doesn't compare them.

This works:	`CASE(custom_field__c, "1", cf2__c, cf3__c))` where either or both `cf2__c` and `cf3__c` are encrypted
Why it works:	`custom_field__c` is compared to "1". If it is true, the formula returns `cf2__c` because it's not comparing two encrypted values.

This doesn’t work:

```
CASE("1", cf1__c, cf2__c, cf3__c)
```

where `cf1__c` is encrypted

Why it doesn’t work: You can’t compare encrypted values.

`ISBLANK` and `ISNULL`

This works:

```
OR(ISBLANK(encryptedField__c), ISNULL(encryptedField__c))
```

Why it works: Both `ISBLANK` and `ISNULL` are supported. `OR` works in this example because `ISBLANK` and `ISNULL` return a Boolean value, not an encrypted value.

Spanning

This works:

```
(LookupObject1__r.City & LookupObject1__r.Street) &
 (LookupObject2__r.City & LookupObject2__r.Street) &
  (LookupObject3__r.City & LookupObject3__r.Street) &
   (LookupObject4__r.City & LookupObject4__r.Street)
```

How and why you use it: Spanning retrieves encrypted data from multiple entities. For example, let’s say you work in the customer service department for Universal Containers. A customer has filed a case about a distribution problem, and you want to see the scope of the issue. You want all the shipping addresses related to this particular case. This example returns all the customers’ shipping addresses as a single string in your case layout.

Validation

The encryption validation service checks your org to make sure that it’s compatible with encrypted formula field types.

When you encrypt a given field, the validation service:

- Retrieves all formula fields that reference the field
- Verifies that the formula fields are compatible with encryption
- Verifies that the formula fields aren’t used elsewhere for filtering or sorting

Limits

Up to 200 formula fields can reference a given encrypted custom field. A field that is referenced by more than 200 formula fields can’t be encrypted. If you need to reference an encrypted custom field from more than 200 formula fields, contact Salesforce.

When you specify multiple fields to encrypt at one time, the 200-field limit is applied to the whole batch. If you know that you are encrypting fields that have multiple formula fields pointing to them, encrypt those fields one at a time.

Important: Beginning in Spring '17, Shield Platform Encryption no longer masks encrypted data. To get the most out of encryption support for custom formula field types, we recommend that you approve the "Turn Off Masking for Encrypted Data" critical update.

To activate this critical update:

1. Review your field-level security settings for any field types that include encrypted data. Ensure that field access is properly set in your org.
2. From Setup, enter `Critical Updates` in the `Quick Find` box and select **Critical Updates**.
3. For Turn Off Masking for Encrypted Data, click **Activate**.
4. Refresh your browser page.

Encrypt Data in Chatter

Enabling Shield Platform Encryption for Chatter adds an extra layer of security to information that users share in Chatter. You can encrypt data at rest in feed posts and comments, questions and answers, link names and URLs, poll questions and choices, and content from your custom rich publisher apps.

To activate encryption for Chatter, contact Salesforce. Once encryption for Chatter is activated, we recommend that you test it in a dedicated Sandbox environment.

Unlike encryption for custom and standard fields, enabling encryption for Chatter encrypts all eligible Chatter fields.

1. To enable access to this feature, first contact Salesforce.
2. Make sure that your org has an active encryption key. If you're not sure, check with your administrator.
3. From Setup, use the Quick Find box to find the Platform Encryption setup page.
4. Click **Encrypt Chatter**.

The automatic Shield Platform Encryption validation service checks for settings that could block encryption. If the service finds potential problems, you're sent an email with suggestions for fixing the problems.

After you activate encryption for Chatter, new data that you enter into Chatter gets encrypted. To encrypt historic Chatter, contact Salesforce.

When you edit or update an encrypted Chatter field, the field's revision history is also encrypted. For example, if you update a post, the old version of the post remains encrypted.

If you enabled Encryption for Chatter in Spring '17 and you want to access the most up-to-date features for this pilot, deselect **Encrypt Chatter** and then reselect **Encrypt Chatter**.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:
- View Setup and Configuration

To encrypt fields:
- Customize Application

Note: This feature is available when you have activated the "Turn Off Masking for Encrypted Data" critical update.

Manage Shield Platform Encryption

To provide Shield Platform Encryption for your organization, contact your Salesforce account executive. They'll help you provision the correct license so you can get started on creating your own unique tenant secret.

Assign the Manage Encryption Keys, Manage Certificates, and Customize Application permissions to people you trust to manage tenant secrets and certificates. Users with the Manage Encryption Keys permission can generate, export, import, and destroy organization-specific keys. It's a good idea to monitor the key management activities of these users regularly with the setup audit trail.

Users with both Manage Certificates and Manage Encryption Keys permissions can manage certificates and tenant secrets with the Shield Platform Encryption Bring Your Own Key (BYOK) service. You can also monitor these users' key and certificate management activities with the setup audit trail.

Authorized developers can generate, rotate, export, destroy, and reimport tenant secrets by coding a call to the TenantSecret object in the Salesforce API.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:
- Manage Encryption Keys

IN THIS SECTION:

Generate a Tenant Secret

You can have Salesforce generate a unique tenant secret for your organization, or you can generate your own tenant secret using your own external resources. In either case, you manage your own tenant secret: you can rotate it, archive it, and designate other users to share responsibility for it.

Rotate Your Encryption Tenant Secrets

You control the life cycle of your data encryption keys by controlling the life cycle of your tenant secrets. It's recommended to regularly generate a new tenant secret and archive the previously active one.

Back Up Your Tenant Secret

Your tenant secret is unique to your organization and to the specific data to which it applies. Salesforce recommends that you export your secret to ensure continued data access in cases where you need to gain access to the related data again.

Destroy A Tenant Secret

Only destroy tenant secrets in extreme cases where access to related data is no longer needed. Your tenant secret is unique to your organization and to the specific data to which it applies. Once you destroy a tenant secret, related data is not accessible unless you previously exported the key and then import the key back into Salesforce.

Turn Shield Platform Encryption Off

At some point, you may need to disable Shield Platform Encryption for fields, files, or both. You can turn field encryption on or off individually, but file encryption is all or nothing.

SEE ALSO:

Platform Encryption Overview

Tenant Secret API

Generate a Tenant Secret

You can have Salesforce generate a unique tenant secret for your organization, or you can generate your own tenant secret using your own external resources. In either case, you manage your own tenant secret: you can rotate it, archive it, and designate other users to share responsibility for it.

When you generate a new tenant secret, any new data is encrypted using this key. However, existing sensitive data remains encrypted using previous keys. In this situation, we strongly recommend re-encrypting these fields using the latest key. Contact Salesforce for help with this.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:
- Manage Encryption Keys

IN THIS SECTION:

Generate a Tenant Secret with Salesforce
Salesforce makes it easy to generate a unique tenant secret from the Setup menu.

Manage Tenant Secrets by Type
Tenant secret types allow you to specify which kind of data you want to encrypt with a tenant secret. You can apply different key rotation cycles or key destruction policies to tenant secrets that encrypt different kinds of data. You can apply a tenant secret to search index files or other data stored in Salesforce.

Generate Your Own Tenant Secret (BYOK)
When you supply your own tenant secret, you get the benefits of built-in Salesforce Shield Platform Encryption plus the extra assurance that comes from exclusively managing your tenant secret.

SEE ALSO:

Permission Sets

Profiles

API Guide: TenantSecret

Generate a Tenant Secret with Salesforce

Salesforce makes it easy to generate a unique tenant secret from the Setup menu.

Only authorized users can generate tenant secrets from the Platform Encryption page. Ask your Salesforce admin to assign you the Manage Encryption Keys permission.

1. From Setup, enter `Platform Encryption` in the `Quick Find` box and select **Platform Encryption**.
2. In the Choose Tenant Secret Type drop-down list, choose a data type.
3. Click **Generate Tenant Secret**.

   How often you can generate a tenant secret depends on the tenant secret type.

   - You can generate tenant secrets for the Data in Salesforce type once every 24 hours in production orgs, and once every 4 hours in Sandbox orgs.
   - You can generate tenant secrets for the Search Index type once every 7 days.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:
- Manage Encryption Keys

Manage Tenant Secrets by Type

Tenant secret types allow you to specify which kind of data you want to encrypt with a tenant secret. You can apply different key rotation cycles or key destruction policies to tenant secrets that encrypt different kinds of data. You can apply a tenant secret to search index files or other data stored in Salesforce.

Tenant secrets are categorized according to the kind of data they encrypt.

- Data in Salesforce, which includes fields, attachments, and files other than search index files
- Search index files

Note: Tenant secrets that were generated or uploaded before the Spring '17 release are categorized as the Data in Salesforce type.

1. From Setup, enter `Platform Encryption` in the `Quick Find` box and select **Platform Encryption**.
2. In the Choose Tenant Secret Type drop-down list, choose a data type.

   The Key Management section displays all tenant secrets of that data type. If you generate or upload a tenant secret while viewing tenant secrets of a particular type, it becomes the active tenant secret for that data.

   To enable search index encryption, contact your Salesforce account executive or open a support ticket.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:
- Manage Certificates

  AND

  Manage Encryption Keys

Generate Your Own Tenant Secret (BYOK)

When you supply your own tenant secret, you get the benefits of built-in Salesforce Shield Platform Encryption plus the extra assurance that comes from exclusively managing your tenant secret.

Controlling your own tenant secret entails generating a BYOK-compatible certificate, using that certificate to encrypt and secure your self-generated tenant secret, then granting the Salesforce Shield Platform Encryption key management machinery access to your tenant secret.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:

- Manage Encryption Keys

  AND

  Manage Certificates

IN THIS SECTION:

1. Generate a BYOK-Compatible Certificate

   Use Salesforce to generate a certificate to encrypt the tenant secret that we'll use to derive your org-specific data encryption key. You can generate a self-signed or certificate-authority (CA) signed certificate.

2. Generate and Wrap Your Tenant Secret

   Generate a random number as your tenant secret. Then calculate an SHA256 hash of the secret, and encrypt it with the public key from the certificate you generated.

3. Upload Your Tenant Secret

   Once you have your tenant secret, upload it to Salesforce so that the Shield Platform Encryption key management machinery can use it to derive your org-specific data encryption key.

Generate a BYOK-Compatible Certificate

Use Salesforce to generate a certificate to encrypt the tenant secret that we'll use to derive your org-specific data encryption key. You can generate a self-signed or certificate-authority (CA) signed certificate.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:

- Manage Encryption Keys

  AND

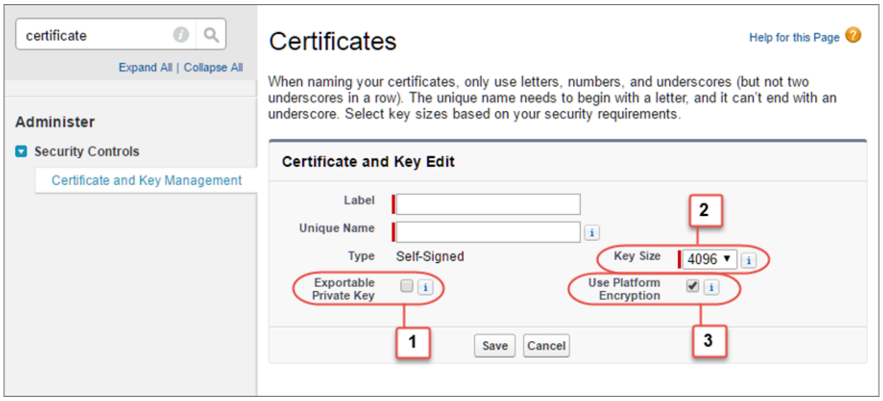
  Manage Certificates

To create a self-signed certificate:

1. In Setup, use the Quick Find box to go to the Platform Encryption page.
2. Click **Upload Tenant Secret**.
3. Click **Create Self-Signed Certificate**.
4. Enter a unique name for your certificate in the Label field. The Unique Name field to automatically assign a name based on what you entered in the Label field.

   The **Exportable Private Key**, **Use Platform Encryption**, and **Key Size** settings are pre-selected. This ensures that your self-signed certificate is compatible with Salesforce Shield Platform Encryption.

   > Important: You can also create a BYOK-compatible self-signed certificate from the Certificate and Key Management page. If you chose this option, you must 1) disable **Exportable Private Key**, 2) specify a 4096-bit certificate size, and 3) enable **Platform Encryption**.



Certificates

When naming your certificates, only use letters, numbers, and underscores (but not two underscores in a row). The unique name needs to begin with a letter, and it can't end with an underscore. Select key sizes based on your security requirements.

Certificate and Key Edit

Label

Unique Name

Type Self-Signed

Key Size 4096

Exportable Private Key ☐

Use Platform Encryption ☑

5. When the Certificate and Key Detail page appears, click **Download Certificate**.

   If you're not sure whether a self-signed or CA-signed certificate is right for you, consult your organization's security policy. See Certificates and Keys in Salesforce Help for more about what each option implies.

   To create a CA-signed certificate, follow the instructions in the Generate a Certificate Signed By a Certificate Authority topic in Salesforce Help. Remember to manually change the **Exportable Private Key**, **Key Size**, and **Platform Encryption** settings to ensure that your certificate is BYOK-compatible.

SEE ALSO:

Certificates and Keys

Generate a Certificate Signed by a Certificate Authority

Generate and Wrap Your Tenant Secret

Generate a random number as your tenant secret. Then calculate an SHA256 hash of the secret, and encrypt it with the public key from the certificate you generated.

1. Generate a 256-bit tenant secret using the method of your choice.

   You can generate your tenant secret in one of two ways:

   - Use your own on-premise resources to generate a tenant secret programmatically, using an open source library such as Bouncy Castle or OpenSSL.

     Tip: We've provided a script on page 528 that may be useful as a guide to the process.

   - Use a key brokering partner that can generate, secure, and share access to your tenant secret.

2. Wrap your tenant secret with the public key from the BYOK-compatible certificate you generated. Specify the OAEP padding scheme. Make sure the resulting encrypted tenant secret and hashed tenant secret files are encoded using base64.

3. Encode this encrypted tenant secret to base64.

4. Calculate an SHA-256 hash of the plaintext tenant secret.

5. Encode the SHA-256 hash of the plaintext tenant secret to base64.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:

- Manage Encryption Keys

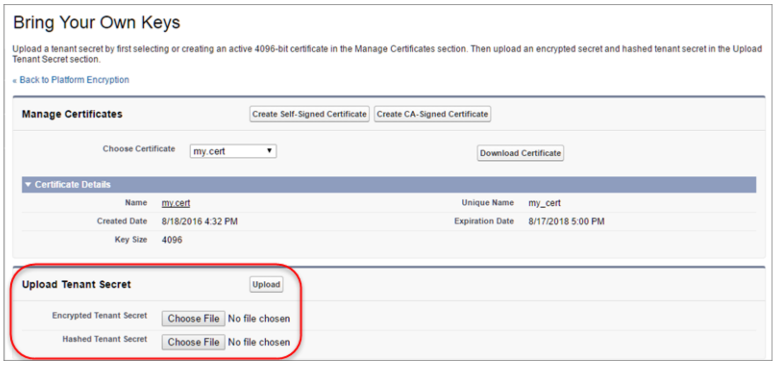
  AND

  Manage Certificates

Upload Your Tenant Secret

Once you have your tenant secret, upload it to Salesforce so that the Shield Platform Encryption key management machinery can use it to derive your org-specific data encryption key.

1. In Setup, use the Quick Find box to go to the Platform Encryption setup page.
2. Click **Upload Tenant Secret**.
3. In the Upload Tenant Secret section, attach both the encrypted tenant secret and the hashed plaintext tenant secret. Click **Upload**.



Bring Your Own Keys

Upload a tenant secret by first selecting or creating an active 4096-bit certificate in the Manage Certificates section. Then upload an encrypted secret and hashed tenant secret in the Upload Tenant Secret section.

« Back to Platform Encryption

Manage Certificates

Choose Certificate: my.cert

Certificate Details

Name	my.cert	Unique Name	my_cert
Created Date	8/18/2016 4:32 PM	Expiration Date	8/17/2018 5:00 PM
Key Size	4096		

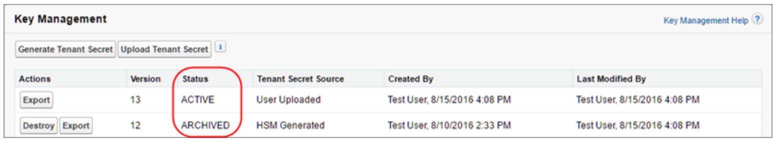
Upload Tenant Secret

Encrypted Tenant Secret: Choose File No file chosen

Hashed Tenant Secret: Choose File No file chosen

This tenant secret automatically becomes the active tenant secret.

Note: The tenant secret whose certificate has the latest expiration date automatically becomes the active tenant secret.



Key Management

Actions	Version	Status	Tenant Secret Source	Created By	Last Modified By
Export	13	ACTIVE	User Uploaded	Test User, 8/15/2016 4:08 PM	Test User, 8/15/2016 4:08 PM
Destroy Export	12	ARCHIVED	HSM Generated	Test User, 8/10/2016 2:33 PM	Test User, 8/15/2016 4:08 PM

Your tenant secret is now ready to be used for key derivation. From here on, the Salesforce key derivation server will use the tenant secret you generated to derive the org-specific key that the app server will use to encrypt and decrypt your users' data.

4. Export your tenant secret and back it up as prescribed in your organization's security policy.

   You'll have to reimport the secret if you need to restore it. The exported secret is different from the key you uploaded. It is encrypted with a different key and has additional metadata embedded in it. See Back Up Your Tenant Secret in the Salesforce Help.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:

- Manage Encryption Keys

  AND

  Manage Certificates

Rotate Your Encryption Tenant Secrets

You control the life cycle of your data encryption keys by controlling the life cycle of your tenant secrets. It's recommended to regularly generate a new tenant secret and archive the previously active one.

Consult your organization's security policies to decide how often to rotate your tenant secrets. You can rotate a tenant secret once every 24 hours in production orgs and every 4 hours in sandbox environments.

The key derivation function uses a master secret, which is rotated with each major Salesforce release. Master secret rotation doesn't impact your encryption keys or your encrypted data until you rotate your tenant secret.

1. From Setup, enter `Platform Encryption` in the Quick Find box, then click **Platform Encryption**.
2. From the Choose Tenant Secret Type dropdown, choose a data type.
3. Check the status of the data type's tenant secrets. Existing tenant secrets are listed as active, archived, or destroyed.

   ACTIVE
   Can be used to encrypt and decrypt new or existing data.

   ARCHIVED
   Can't encrypt new data. Can be used to decrypt data previously encrypted with this key when it was active.

   DESTROYED
   Can't encrypt or decrypt data. Data encrypted with this key when it was active can no longer be decrypted. Files and attachments encrypted with this key can no longer be downloaded.

4. Click **Generate New Tenant Secret** or **Upload Tenant Secret**. If uploading a customer-supplied tenant secret, upload your encrypted tenant secret and tenant secret hash.
5. If you want to re-encrypt field values with a newly generated tenant secret, contact Salesforce support.

   To update your data, export the objects via the API or run a report that includes the record ID. These actions trigger the encryption service to encrypt the existing data again using the newest key.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

SEE ALSO:

API Guide: TenantSecret

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:

- Manage Encryption Keys

Back Up Your Tenant Secret

Your tenant secret is unique to your organization and to the specific data to which it applies. Salesforce recommends that you export your secret to ensure continued data access in cases where you need to gain access to the related data again.

1. In Setup, use the `Quick Find` box to find the Platform Encryption setup page.
2. In the table that lists your keys, find the tenant secret you want and click **Export**.
3. Confirm your choice in the warning box, then save your exported file.

   The file name is `tenant-secret-org-<organization ID>-ver-<tenant secret version numer>.txt`. For example, `tenant-secret-org-00DD00000007eTR-ver-1.txt`.
4. Note the specific version you're exporting, and give the exported file a meaningful name. Store the file in a safe location in case you need to import it back into your organization.

   Note: Your exported tenant secret is itself encrypted.
5. To import your tenant secret again, click **Import** > **Choose File** and select your file. Make sure you're importing the correct version of the tenant secret.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:
- Manage Encryption Keys

SEE ALSO:

API Guide: TenantSecret

Destroy A Tenant Secret

Only destroy tenant secrets in extreme cases where access to related data is no longer needed. Your tenant secret is unique to your organization and to the specific data to which it applies. Once you destroy a tenant secret, related data is not accessible unless you previously exported the key and then import the key back into Salesforce.

You are solely responsible for making sure your data and tenant secrets are backed up and stored in a safe place. Salesforce can't help you with deleted, destroyed, or misplaced tenant secrets.

1. In Setup, use the `Quick Find` box to find the Platform Encryption setup page.
2. In the table that lists your tenant secrets, go to the row that contains the one you want to destroy and click **Destroy**.
3. A warning box appears. Type in the text as shown and select the checkbox acknowledging that you're destroying a tenant secret, then click **Destroy**.

File previews and content that was already cached in the user's browser may still be visible in cleartext after you destroy the key that encrypted that content, until the user logs in again.

If you create a sandbox organization from your production organization and then destroy the tenant secret in your sandbox organization, the tenant secret still exists in the production organization.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To manage tenant secrets:
- Manage Encryption Keys

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

SEE ALSO:

API Guide: TenantSecret

Turn Shield Platform Encryption Off

At some point, you may need to disable Shield Platform Encryption for fields, files, or both. You can turn field encryption on or off individually, but file encryption is all or nothing.

When you turn off Shield Platform Encryption, encrypted data is not mass-decrypted and any functionality that is affected by encryption is not restored. Contact Salesforce after disabling Platform Encryption for help finalizing your changes.

1. From Setup, use the `Quick Find` box to find **Platform Encryption**.
2. Click **Encrypt Fields**, then click **Edit**.
3. Deselect the fields you want to stop encrypting, then click **Save**.
   Users can see data in these fields.
4. To disable encryption for files, deselect **Encrypt Files and Attachments** and click **Save**.

The limitations and special behaviors that apply to encrypted fields persist after encryption is disabled. Any previously encrypted files and attachments may remain encrypted at rest.

Encrypted fields remain accessible after you disable encryption, as long as the key used to encrypt them has not been destroyed.

SEE ALSO:

Back to Parent Topic

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:

- View Setup and Configuration

To disable encryption:

- Customize Application

How Shield Platform Encryption Works

Shield Platform Encryption relies on a unique tenant secret that you control and a master secret that's maintained by Salesforce. We combine these secrets to create your unique data encryption key. We use that key to encrypt data that your users put into Salesforce, and to decrypt data when your authorized users need it.

Encrypting files, fields, and attachments has no effect on your organization's storage limits.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

IN THIS SECTION:

Can I Bring My Own Encryption Key?

Yes. You can generate and store your tenant secret outside of Salesforce using your own crypto libraries, enterprise key management system, or hardware security module (HSM). You then grant the Salesforce Shield Platform Encryption key management machinery access to those keys. You can choose to encrypt your keys with a public key from a self-signed or CA-signed certificate.

Which Standard Fields Can I Encrypt?

You can encrypt certain fields on standard objects, on custom objects, and in Chatter. With some exceptions, encrypted fields work normally throughout the Salesforce user interface, business processes, and APIs.

Which Custom Fields Can I Encrypt?

You can encrypt the contents of fields that belong to one these custom field types, on either standard or custom objects.

Which Files Are Encrypted?

When you enable Shield Platform Encryption for files and attachments, all files and attachments that can be encrypted are encrypted. The body of each file or attachment is encrypted when it's uploaded.

Which User Permissions Does Shield Platform Encryption Require?

Assign permissions to your users according to their roles regarding encryption and key management. Some users need permission to select data for encryption, while other users require combinations of permissions to work with certificates or tenant secrets. You can enable these permissions for user profiles just like you would any other user permission.

Why Isn't My Encrypted Data Masked?

If the encryption service isn't available, data is masked in some types of encrypted fields. This is to help you troubleshoot encryption key issues, not to control user access to data. If you have data that you don't want some users to see, revisit those users' field-level security settings, record access settings, and object permissions.

Behind the Scenes: The Shield Platform Encryption Process

When users submit data, the application server looks for the org-specific data encryption key in its cache. If it isn't there, the application server gets the encrypted tenant secret from the database and asks the key derivation server to derive the key. The encryption service then encrypts the data on the application server.

Behind the Scenes: The Search Index Encryption Process

The Salesforce search engine is built on the open-source enterprise search platform software Apache Solr. The search index, which stores tokens of record data with links back to the original records stored in the database, is housed within Solr. Partitions divide the search index into segments to allow Salesforce to scale operations. Apache Lucene is used for its core library.

How Do I Deploy Shield Platform Encryption?

When you deploy Shield Platform Encryption to your organization with a tool such as Force.com IDE, Migration Tool, or Workbench, the Encrypted field attribute persists. However, if you deploy to organizations with different encryption settings, the effect depends on whether Shield Platform Encryption is enabled in the target organization.

How Does Shield Platform Encryption Work In a Sandbox?

Refreshing a sandbox from a production organization creates an exact copy of the production organization. If Shield Platform Encryption is enabled on the production organization, all encryption settings are copied, including tenant secrets created in production.

Shield Platform Encryption Terminology

Encryption has its own specialized vocabulary. To get the most out of your Shield Platform Encryption features, it's a good idea to familiarize yourself with the key terms, such as hardware security module, key rotation, and master secret.

What’s the Difference Between Classic Encryption and Shield Platform Encryption?

With Shield Platform Encryption, you can encrypt a variety of widely used standard fields, along with some custom fields and many kinds of files. Shield Platform Encryption also supports person accounts, cases, search, approval processes, and other key Salesforce features. Classic encryption lets you protect only a special type of custom text field, which you create for that purpose.

SEE ALSO:

Platform Encryption Overview

https://resources.docs.salesforce.com/202/latest/en-us/sfdc/pdf/salesforce_platform_encryption_implementation_guide.pdf

Can I Bring My Own Encryption Key?

Yes. You can generate and store your tenant secret outside of Salesforce using your own crypto libraries, enterprise key management system, or hardware security module (HSM). You then grant the Salesforce Shield Platform Encryption key management machinery access to those keys. You can choose to encrypt your keys with a public key from a self-signed or CA-signed certificate.

To work with our key management machinery, your tenant secret needs to meet these specifications:

- 256-bit size
- Encrypted with a public RSA key that is extracted from the downloaded BYOK certificate, then padded using OAEP padding
- Once it’s encrypted, it must be encoded in standard base64

To work with encryption keys, you'll need the “Manage Encryption Keys” permission. To generate BYOK-compatible certificates, you’ll need the “Customize Application” permission.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer ’15 and later.

Available in both Salesforce Classic and Lightning Experience.

IN THIS SECTION:

Why Bring Your Own Key?

Bring Your Own Key (BYOK) gives you an extra layer of protection in the event of unauthorized access to critical data. It may also help you meet the regulatory requirements that come with handling financial data, such as credit card numbers; health data, such as patient care records or insurance information; or other kinds of private data, such as social security numbers, addresses, and phone numbers. Once you’ve set up your key, you can use Shield Platform Encryption as you normally would to encrypt data at rest in your Salesforce org.

Take Good Care of Your Keys

When you create and store your own key material outside of Salesforce, it’s important that you safeguard those tenant secrets. Make sure that you have a trustworthy place to archive your tenant secret; never save a tenant secret on a hard drive without a backup.

Sample Script for Generating a BYOK Tenant Secret

We’ve provided a helper script that may be handy for preparing your tenant secret for installation. It generates a random number as your tenant secret, calculates a SHA256 hash of the secret, and uses the public key from the certificate to encrypt the secret.

Troubleshooting Bring Your Own Key

One or more of these frequently asked questions may help you troubleshoot any problems that arise.

Why Bring Your Own Key?

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Bring Your Own Key (BYOK) gives you an extra layer of protection in the event of unauthorized access to critical data. It may also help you meet the regulatory requirements that come with handling financial data, such as credit card numbers; health data, such as patient care records or insurance information; or other kinds of private data, such as social security numbers, addresses, and phone numbers. Once you've set up your key, you can use Shield Platform Encryption as you normally would to encrypt data at rest in your Salesforce org.

Shield Platform Encryption enables Salesforce administrators to manage the lifecycle of their data encryption keys while protecting these keys from unauthorized access. By controlling the lifecycle of your organization's tenant secrets, you control the lifecycle of the data encryption keys derived from them.

Data encryption keys aren't stored in Salesforce. Instead, they're derived on demand whenever a key is needed to encrypt or decrypt customer data, using a master secret and a tenant secret. The master secret is generated once per release for everyone by a hardware security module (HSM). The tenant secret is unique to your organization, and you control when it is generated, activated, and retired.

You can generate your tenant secrets in two ways:

- Use the Salesforce hardware security module (HSM) key management infrastructure to have your org-specific tenant secret generated for you.
- Use the infrastructure of your choice, such as an on-premise HSM, to generate and manage your tenant secret. This option is popularly known as "Bring Your Own Key," although the element you're really bringing is the tenant secret from which the key is derived.

Take Good Care of Your Keys

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

When you create and store your own key material outside of Salesforce, it's important that you safeguard those tenant secrets. Make sure that you have a trustworthy place to archive your tenant secret; never save a tenant secret on a hard drive without a backup.

Back up all imported tenant secrets after you upload them to Salesforce to ensure that you have copies of your active tenant secrets. See Back Up Your Tenant Secret in the Salesforce Help.

Review your company policy on key rotation. You can rotate and update your keys on your own schedule. See Rotate Your Encryption Keys.

Important: If you accidentally destroy a tenant secret that isn't backed up, Salesforce won't be able to help you retrieve it.

Sample Script for Generating a BYOK Tenant Secret

We've provided a helper script that may be handy for preparing your tenant secret for installation. It generates a random number as your tenant secret, calculates a SHA256 hash of the secret, and uses the public key from the certificate to encrypt the secret.

1. Download the script from the Salesforce Knowledge Base. Save it in the same directory as the certificate.
2. Run the script specifying the certificate name, like this: `./secretgen.sh my_certificate.crt`

   Replace this certificate name with the actual filename of the certificate you downloaded.

   Tip: If needed, use `chmod +w secretgen.sh` to make sure you have write permission to the file and use `chmod 775` to make it executable.
3. The script generates a number of files. Look for the two files that end with the .b64 suffix. The files ending in .b64 are your base 64-encoded encrypted tenant secret and base 64-encoded hash of the plaintext tenant secret. You'll need both of these files for the next step.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Troubleshooting Bring Your Own Key

One or more of these frequently asked questions may help you troubleshoot any problems that arise.

I'm trying to use the script you provide, but it won't run.

Make sure that you are running the right script for your operating system. If you are working on a Windows machine, you can install a Linux emulator and use the Linux script. These issues can also prevent the script from running:

- You don't have write permission in the folder you're trying to run the script from. Try running the script from a folder that you have write permission for.
- The certificate that the script references is missing. Make sure you've properly generated the certificate.
- The certificate is missing or is not being referenced by the correct name. Make sure you've entered the correct file name for your certificate in the script.

I want to use the script you provide, but I also want to use my own random number generator.

The script we provide uses a random number generator to create a random value that is then used as your tenant secret. If you would like to use a different generator, replace `head -c 32 /dev/urandom | tr '\n' =` (or, in the Mac version, `head -c 32 /dev/urandom > $PLAINTEXT_SECRET`) with a command that generates a random number using your preferred generator.

What if I want to use my own hashing process to hash my tenant secret?

No problem. Just make sure that the end result meets these requirements:

- Uses an SHA-256 algorithm.
- Results in a base64 encoded hashed tenant secret.
- Generates the hash of the random number BEFORE encrypting it.

If any of these three criteria aren't met, you won't be able to upload your tenant secret.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

How should I encrypt my tenant secret before I upload it to Salesforce?

If you're using the script provided, the encryption process is taken care of. If you do not use the script, specify the OAEP padding scheme when you encrypt your tenant secret. Make sure the resulting encrypted tenant secret and hashed tenant secret files are encoded using base64. If either of these criteria are not met, you won't be able to upload your tenant secret.

If you choose to not use the script provided, follow the instructions in the Generate And Wrap Your Tenant Secret Help topic.

I can't upload my Encrypted tenant secret and Hashed tenant secret.

A handful of errors can prevent your files from uploading. Use the chart to make that sure your tenant secrets and certificates are in order.

Possible cause	Solution
Your files were generated with an expired certificate.	Check the date on your certificate. If it has expired, you can renew your certificate or use another one.
Your certificate is not active, or is not a valid Bring Your Own Key certificate.	Ensure that your certificate settings are compatible with the Bring Your Own Key feature. Under the Certificate and Key Edit section of the Certificates page, select a 4096-bit certificate size, disable Exportable Private Key, and enable Platform Encryption.
You haven't attached both the encrypted tenant secret and the hashed tenant secret.	Make sure that you attach both the encrypted tenant secret and hashed tenant secret. Both of these files should have a .b64 suffix.
Your tenant secret or hashed tenant secret wasn't generated properly.	Several problems can cause this error. Usually, the tenant secret or hashed tenant secret wasn't generated using the correct SSL parameters. If you are using OpenSSL, you can refer to the script for an example of the correct parameters you should use to generate and hash your tenant secret. If you are using a library other than OpenSSL, check that library's support page for help finding the correct parameters to both generate and hash your tenant secret. Still stuck? Contact your Salesforce account executive. They'll put you in touch with someone at Salesforce who can help.

I'm still having problems with my key. Who should I talk to?

If you still have questions, contact your account executive. They'll put you in touch with a support team specific to this feature.

Which Standard Fields Can I Encrypt?

You can encrypt certain fields on standard objects, on custom objects, and in Chatter. With some exceptions, encrypted fields work normally throughout the Salesforce user interface, business processes, and APIs.

Note: Beginning with Spring '17, Shield Platform Encryption no longer masks encrypted data in the presentation layer. This may affect some users' ability to work with encrypted data. If you have data you don't want specific users to see, revisit their field-level security settings on page 312, record access settings, and object permissions on page 315.

When you encrypt a field, existing values aren't encrypted immediately. Values are encrypted only after they are touched. Contact Salesforce for help encrypting existing data.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Encrypted Standard Fields

You can encrypt the contents of these standard field types.

Accounts (Business)

- `Account Name`
- `Billing`
- `Description`
- `Fax`
- `Website`
- `Phone`
- `Shipping` (encrypts `Street` and `City`)
- `Site`

Person Accounts

- `Name` (Encrypts `First Name`, `Middle Name`, and `Last Name`)
- `Mailing City`

Contacts

- `Assistant`
- `Description`
- `Email`
- `Fax`
- `Home Phone`
- `Mailing Address` (Encrypts `Mailing Street` and `Mailing City`)
- `Mobile`
- `Name` (Encrypts `First Name`, `Middle Name`, and `Last Name`)
- `Other Address` (encrypts `Street` and `City`)
- `Other Phone`
- `Phone`
- `Postal Code`
- `Title`

Cases

- `Subject`
- `Description`

Case Comments

- `Body` (including internal comments)

Leads

- `Address` (Encrypts `Street` and `City`)
- `Company`
- `Description`
- `Email`
- `Fax`
- `Mobile Phone`
- `Name` (Encrypts `First Name`, `Middle Name`, and `Last Name`)
- `Phone`
- `Title`
- `Website`

Chatter feed

- `Feed Comment—Body`
- `Feed Item—Body`
- `Feed Item—Title`
- `Feed Revision—Value`

These fields include feed posts, questions and answers, link names, comments, and poll questions. They don't encrypt poll choices.

The revision history of encrypted Chatter fields is also encrypted. If you edit or update an encrypted Chatter field, the old information remains encrypted.

Note: Enabling Encryption for Chatter encrypts all eligible Chatter fields. You can't choose to encrypt only certain Chatter fields.

SEE ALSO:

Encrypt New Data in Fields
Back to Parent Topic
Why Isn't My Encrypted Data Masked?
Use Encrypted Data in Formulas
Fix Compatibility Problems
Tradeoffs and Limitations of Shield Platform Encryption
Enable Enhanced Lookups

Which Custom Fields Can I Encrypt?

You can encrypt the contents of fields that belong to one these custom field types, on either standard or custom objects.

- Email

- Phone
- Text
- Text Area
- Text Area (Long)
- URL
- Date
- Date/Time

After a custom field is encrypted, you can't change the field type. For custom phone and email fields, you also can't change the field format.

Important: When you encrypt the Name field, enhanced lookups are automatically enabled. Enhanced lookups improve the user's experience by searching only through records that have been looked up recently, and not all existing records. Switching to enhanced lookups is a one-way change. You can't go back to standard lookups, even if you disable encryption.

You can't use Schema Builder to create an encrypted custom field.

Some custom fields can't be encrypted:

- Fields that have the `Unique` or `External ID` attributes or include these attributes on previously encrypted custom fields
- Fields on external data objects
- Fields that are used in an account contact relation

On a custom object, the standard Name field can't be encrypted.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

SEE ALSO:

Encrypt New Data in Fields

Back to Parent Topic

Why Isn't My Encrypted Data Masked?

Use Encrypted Data in Formulas

Fix Compatibility Problems

Tradeoffs and Limitations of Shield Platform Encryption

Enable Enhanced Lookups

Which Files Are Encrypted?

When you enable Shield Platform Encryption for files and attachments, all files and attachments that can be encrypted are encrypted. The body of each file or attachment is encrypted when it's uploaded.

These kinds of files are encrypted when you enable file encryption:

- Files attached to email
- Files attached to feeds
- Files attached to records
- Images included in Rich Text Area fields
- Files on the Content, Libraries, and Files tabs (Salesforce Files, including file previews, and Salesforce CRM Content files)
- Files managed with Salesforce Files Sync and stored in Salesforce
- Files attached to Chatter posts, comments, and the sidebar
- Notes body text using the new Notes tool
- Files attached to Knowledge articles
- Quote PDFs

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

SEE ALSO:

Encrypt New Files and Attachments

Which User Permissions Does Shield Platform Encryption Require?

Assign permissions to your users according to their roles regarding encryption and key management. Some users need permission to select data for encryption, while other users require combinations of permissions to work with certificates or tenant secrets. You can enable these permissions for user profiles just like you would any other user permission.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

	Manage Encryption Keys	Customize Application	View Setup and Configuration	Manage Certificates
View Platform Encryption Setup page		✓	✓	
Edit Platform Encryption setup Page, excluding tenant secret and certificate management		✓		
Generate, destroy, export, and import tenant secrets	✓			
Query TenantSecret object via the API	✓			
Edit, upload, and download HSM-protected certificates with the	✓			✓

	Manage Encryption Keys	Customize Application	View Setup and Configuration	Manage Certificates
Shield Platform Encryption Bring Your Own Key service				

The Customize Application and Manage Certificates permissions are automatically enabled for users with the System Administrator profile.

Note: Beginning with Spring ’17, Shield Platform Encryption no longer masks encrypted data in the presentation layer. This may affect some users’ ability to work with encrypted data. If you have data you don’t want specific users to see, revisit their field-level security settings on page 312, record access settings, and object permissions on page 315.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

SEE ALSO:

Profiles

Permission Sets

User Permissions

Back to Parent Topic

Why Isn’t My Encrypted Data Masked?

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer ’15 and later.

Available in both Salesforce Classic and Lightning Experience.

If the encryption service isn’t available, data is masked in some types of encrypted fields. This is to help you troubleshoot encryption key issues, not to control user access to data. If you have data that you don’t want some users to see, revisit those users’ field-level security settings, record access settings, and object permissions.

Encryption prevents outsiders from using your Salesforce data even if they manage to get it. It is not a way to hide data from authenticated users. User permissions are the only way to control data visibility for authenticated users. Encryption at rest is about logins, not permissions.

With Shield Platform Encryption, if a user is authorized to see a given set of data, that user sees that data whether it’s encrypted or not.

- Authentication means that making sure only legitimate users can get into your system. For example, a company’s Salesforce org is only for use by active employees of that company. Anyone who is not an employee is not authenticated; that is, they are barred from logging in. If they do somehow get their hands on the data, it’s useless to them because it is encrypted.
- Authorization defines which data or features an authenticated user can use. For example, a sales associate can see and use data in the Leads object, but can’t see the regional forecasts, which are intended for sales managers. Both the associate and the manager are properly logged in (authenticated), but their permissions (authorization) are different. That the data is encrypted doesn’t make any difference to them.

In general, data can be masked but not encrypted, or encrypted but not masked. For example, regulators often require that only the last four digits of a credit card number be visible to users. Applications typically mask the rest of the number, meaning they replace the digits with asterisks on the user’s screen. Without encryption, you can still read the digits that are masked if you can get to the database where they are stored.

Masking might not be enough for your credit card numbers. You may or may not want to encrypt them in the database as well. (You probably should.) If you do, authenticated users will still see the same masked values.

In this way, masking and encryption are different solutions for different problems. You mask data to hide it from users who are authenticated but not authorized to see that data. You encrypt data to prevent someone from stealing the data. (Or, more precisely, to make the data useless if someone does steal it.)

The following table shows the fields that use masking. All others don't.

Field Type	Mask	What It Means
Email, Phone, Text, Text Area, Text Area (Long), URL	?????	This field is encrypted, and the encryption key has been destroyed.
	!!!!!	This service is unavailable right now. For help accessing this service, contact Salesforce.
Custom Date	08/08/1888	This field is encrypted, and the encryption key has been destroyed.
	01/01/1777	This service is unavailable right now. For help accessing this service, contact Salesforce.
Custom Date/Time	08/08/1888 12:00 PM	This field is encrypted, and the encryption key has been destroyed.
	01/01/1777 12:00 PM	This service is unavailable right now. For help accessing this service, contact Salesforce.

You can't enter these masking characters into an encrypted field. For example, if a Date field is encrypted and you enter 07/07/1777, you must enter a different value before it can be saved.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

Behind the Scenes: The Shield Platform Encryption Process

When users submit data, the application server looks for the org-specific data encryption key in its cache. If it isn't there, the application server gets the encrypted tenant secret from the database and asks the key derivation server to derive the key. The encryption service then encrypts the data on the application server.

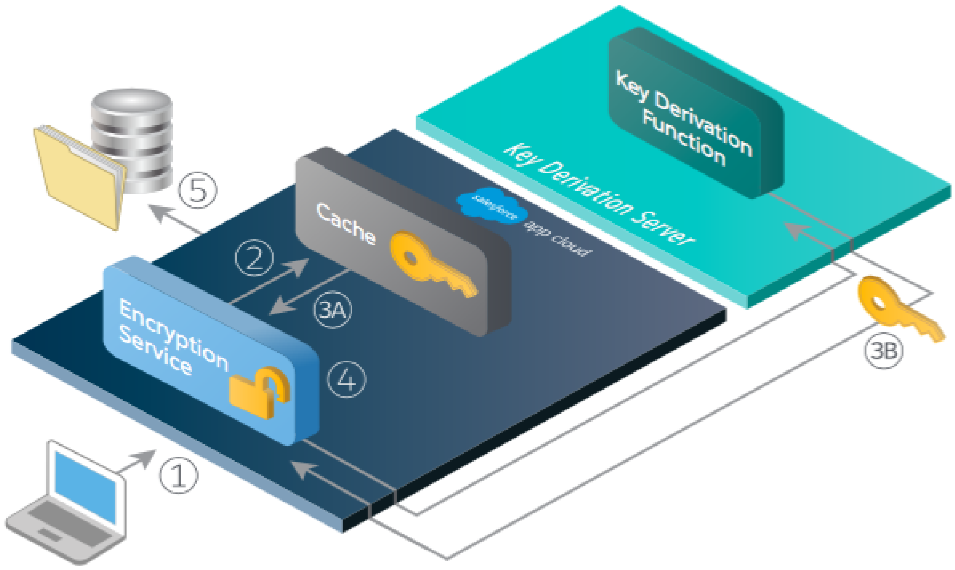
Salesforce securely generates the master and tenant secrets by using Hardware Security Modules (HSMs). The unique key is derived by using PBKDF2, a Key Derivation Function (KDF), with the master and tenant secrets as inputs.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Shield Platform Encryption Process Flow



1. When a Salesforce user saves encrypted data, the runtime engine determines from metadata whether to encrypt the field, file, or attachment before storing it in the database.
2. If so, the encryption service checks for the matching data encryption key in cached memory.
3. The encryption service determines whether the key exists.
   a. If so, the encryption service retrieves the key.
   b. If not, the service sends a derivation request to a key derivation server and returns it to the encryption service running on the Salesforce Platform.
4. After retrieving or deriving the key, the encryption service generates a random initialization vector (IV) and encrypts the data using 256-bit AES encryption.
5. The ciphertext is saved in the database or file storage. The IV and corresponding ID of the tenant secret used to derive the data encryption key are saved in the database.

Salesforce generates a new master secret at the start of each release.

SEE ALSO:

Back to Parent Topic

Shield Platform Encryption Terminology

Salesforce Platform Encryption Architecture

Video: Shield Platform Encryption (Lightning Experience)

Behind the Scenes: The Search Index Encryption Process

The Salesforce search engine is built on the open-source enterprise search platform software Apache Solr. The search index, which stores tokens of record data with links back to the original records stored in the database, is housed within Solr. Partitions divide the search index into segments to allow Salesforce to scale operations. Apache Lucene is used for its core library.

Note: Open a support ticket to enable Search Index Encryption.

Leveraging Shield Platform Encryption's HSM-based key derivation architecture, metadata, and configurations, Search Index Encryption runs when Shield Platform Encryption is in use. The solution applies strong encryption on an org-specific search index (.fdt, .tim, and .tip file types) using an org-specific AES-256 bit encryption key. The search index is encrypted at the search index segment level, and all search index operations require index blocks to be encrypted in memory.

There aren't any changes in Setup or changes to the user interface, so the added protection is seamless and determined by the organization's encryption policy.

The only way to access the search index or the key cache is through programmatic APIs.

Before the search index files are encrypted, a Salesforce security administrator must enable Search Index Encryption. Admins then set up their encryption policy to determine which data elements need to be embedded with encryption. Admins configure Shield Platform Encryption by selecting fields and files to encrypt. An org-specific HSM-derived key specifically for search index encryption is derived on-demand from the tenant secret. The key material is passed to the search engine's cache on a secure channel.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

The process when a user creates or edits records:

1. The core application determines if the search index segment should be encrypted or not based on metadata.
2. If the search index segment should be encrypted, the encryption service checks for the matching search encryption key ID in the cached memory.
3. The encryption service determines if the key exists in the cache.
   a. If the key exists in the cache, the encryption service uses the key for encryption.
   b. Otherwise, the service sends a request to the core application, which in turn sends an authenticated derivation request to a key derivation server and returns the key to the core application server.
4. After retrieving the key, the encryption service generates a random initialization vector (IV) and encrypts the data using NSS or JCE's AES-256 implementation.
5. The key ID (identifier of the key being used to encrypt the index segment) and IV are saved in the search index.

The process is similar when a user searches for encrypted data:

1. When a user searches for a term, the term is passed to the search index, along with which Salesforce objects to search.
2. When the search index executes the search, the encryption service opens the relevant segment of the search index in memory and reads the key ID and IV.
3. Steps 3 through 5 of the process when a user creates or edits records are repeated.
4. The search index processes the search and returns the results to the user seamlessly.

If Salesforce admins disable encryption on a field, all index segments that were encrypted are unencrypted and the key ID is set to null. This process can take up to seven days.

How Do I Deploy Shield Platform Encryption?

When you deploy Shield Platform Encryption to your organization with a tool such as Force.com IDE, Migration Tool, or Workbench, the Encrypted field attribute persists. However, if you deploy to organizations with different encryption settings, the effect depends on whether Shield Platform Encryption is enabled in the target organization.

You can use change sets to deploy Shield Platform Encryption to custom fields. Regardless of how you deploy, Salesforce automatically checks to see if the implementation violates Shield Platform Encryption guidelines.

Source Organization	Target Organization	Result
Shield Platform Encryption enabled	Shield Platform Encryption enabled	The source Encrypted field attribute indicates enablement
Shield Platform Encryption enabled	Shield Platform Encryption not enabled	The Encrypted field attribute is ignored
Shield Platform Encryption not enabled	Shield Platform Encryption enabled	The target Encrypted field attribute indicates enablement

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

SEE ALSO:

Back to Parent Topic

Change Sets

How Does Shield Platform Encryption Work In a Sandbox?

Refreshing a sandbox from a production organization creates an exact copy of the production organization. If Shield Platform Encryption is enabled on the production organization, all encryption settings are copied, including tenant secrets created in production.

Once a sandbox is refreshed, tenant secret changes are confined to your current organization. This means that when you rotate or destroy a tenant secret on sandbox, it doesn't affect the production organization.

As a best practice, rotate tenant secrets on sandboxes after a refresh. Rotation ensures that production and sandbox use different tenant secrets. Destroying tenant secrets on a sandbox renders encrypted data unusable in cases of partial or full copies.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

SEE ALSO:

Back to Parent Topic

Shield Platform Encryption Terminology

Encryption has its own specialized vocabulary. To get the most out of your Shield Platform Encryption features, it's a good idea to familiarize yourself with the key terms, such as hardware security module, key rotation, and master secret.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Data Encryption

The process of applying a cryptographic function to data that results in ciphertext. The platform encryption process uses symmetric key encryption and a 256-bit Advanced Encryption Standard (AES) algorithm using CBC mode, PKCS5 padding, and a randomized, 128-bit initialization vector (IV) to encrypt field-level data and files stored on the Salesforce platform. Both data encryption and decryption occur on the application servers.

Data Encryption Keys

Shield Platform Encryption uses data encryption keys to encrypt and decrypt data. Data encryption keys are derived on a key derivation server using keying material split between a per-release master secret and an organization-specific tenant secret stored encrypted in the database as a part of your organization. The 256-bit derived keys exist in memory until evicted from the cache.

Encrypted Data at Rest

Data that is encrypted when stored on disk. Salesforce supports encryption for fields stored in the database, documents stored in Files, Content Libraries, and Attachments, and archived data.

Encryption Key Management

Refers to all aspects of key management, such as key creation, processes, and storage. Tenant secret management is performed by administrators or users who have the "Manage Encryption Keys" permission.

Hardware Security Module (HSM)

Used to provide cryptography processing as well as key management for authentication. Shield Platform Encryption uses HSMs to generate and store secret material and run the function that derives data encryption keys used by the encryption service to encrypt and decrypt data.

Initialization Vector (IV)

A random sequence used with a key to encrypt data.

Key Derivation Function (KDF)

Uses a pseudorandom number generator and input such as a password to derive keys. Shield Platform Encryption uses PBKDF2 (Password-based Key Derivation Function 2) with HMAC-SHA-256.

Key (Tenant Secret) Rotation

The process of generating a new tenant secret and archiving the previously active one. Active tenant secrets are used for both encryption and decryption. Archived ones are used only for decryption until all data has been re-encrypted using the new, active tenant secret.

Master HSM

The master HSM consists of a USB device used to generate secure, random secrets each Salesforce release. The master HSM is "air-gapped" from Salesforce's production network and stored securely in a bank safety deposit box.

Master Secret

Used in conjunction with the tenant secret and key derivation function to generate a derived data encryption key. The master secret is updated each release by Salesforce and encrypted using the per-release master wrapping key, which is in turn encrypted with the Key Derivation Servers' public key so it can be stored encrypted on the file system. Only HSMs can decrypt it. *No Salesforce employees have access to these keys in cleartext.*

Master Wrapping Key

A symmetric key is derived and used as a master wrapping key, also known as a key wrapping key, encrypting all the per-release keys and secrets bundle.

Tenant Secret

An organization-specific secret used in conjunction with the master secret and key derivation function to generate a derived data encryption key. When an organization administrator rotates a key, a new tenant secret is generated. To access the tenant secret via the API, refer to the TenantSecret object. *No Salesforce employees have access to these keys in cleartext.*

SEE ALSO:

Back to Parent Topic

Behind the Scenes: The Shield Platform Encryption Process

Platform Encryption White Paper

What's the Difference Between Classic Encryption and Shield Platform Encryption?

With Shield Platform Encryption, you can encrypt a variety of widely used standard fields, along with some custom fields and many kinds of files. Shield Platform Encryption also supports person accounts, cases, search, approval processes, and other key Salesforce features. Classic encryption lets you protect only a special type of custom text field, which you create for that purpose.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Feature	Classic Encryption	Platform Encryption
Pricing	Included in base user license	Additional fee applies
Encryption at Rest	✓	✓
Native Solution (No Hardware or Software Required)	✓	✓
Encryption Algorithm	128-bit Advanced Encryption Standard (AES)	256-bit Advanced Encryption Standard (AES)
HSM-based Key Derivation		✓
Manage Encryption Keys Permission		✓
Generate, Export, Import, and Destroy Keys	✓	✓
PCI-DSS L1 Compliance	✓	✓
Masking	✓	
Mask Types and Characters	✓	
View Encrypted Data Permission Required to Read Encrypted Field Values	✓	
Encrypted Standard Fields		✓
Encrypted Attachments, Files, and Content		✓

Feature	Classic Encryption	Platform Encryption
Encrypted Custom Fields	Dedicated custom field type, limited to 175 characters	✓
Encrypt Existing Fields for Supported Custom Field Types		✓
Search (UI, Partial Search, Lookups, Certain SOSL Queries)		✓
API Access	✓	✓
Available in Workflow Rules and Workflow Field Updates		✓
Available in Approval Process Entry Criteria and Approval Step Criteria		✓

Note: Beginning with Spring '17, Shield Platform Encryption no longer masks encrypted data in the presentation layer. This may affect some users' ability to work with encrypted data. If you have data you don't want specific users to see, revisit their field-level security settings on page 312, record access settings, and object permissions on page 315.

SEE ALSO:

Which Standard Fields Can I Encrypt?

Which Custom Fields Can I Encrypt?

Which Files Are Encrypted?

Classic Encryption for Custom Fields

Strengthen Your Data's Security with Shield Platform Encryption

Back to Parent Topic

Strengthen Your Data's Security with Shield Platform Encryption

Classic Encryption for Custom Fields

Platform Encryption Best Practices

Take the time to identify the most likely threats to your organization. This will help you distinguish data that needs encryption from data that doesn't, so that you can encrypt only what you need to. Make sure that your tenant secret and keys are backed up, and be careful who you allow to manage your secrets and keys.

Note: Beginning with Spring '17, Shield Platform Encryption no longer masks encrypted data in the presentation layer. This may affect some users' ability to work with encrypted data. If you have data you don't want specific users to see, revisit their field-level security settings on page 312, record access settings, and object permissions on page 315.

1. Define a threat model for your organization.

   Walk through a formal threat modeling exercise to identify the threats that are most likely to affect your organization. Use your findings to create a data classification scheme, which can help you decide what data to encrypt.

2. Encrypt only where necessary.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

- Not all data is sensitive. Focus on information that requires encryption to meet your regulatory, security, compliance, and privacy requirements. Unnecessarily encrypting data impacts functionality and performance.
- Evaluate your data classification scheme early and work with stakeholders in security, compliance, and business IT departments to define requirements. Balance business-critical functionality against security and risk measures and challenge your assumptions periodically.

3. Create a strategy early for backing up and archiving keys and data.

   If your tenant secrets are destroyed, reimport them to access your data. You are solely responsible for making sure that your data and tenant secrets are backed up and stored in a safe place. Salesforce cannot help you with deleted, destroyed, or misplaced tenant secrets.

4. Read the Shield Platform Encryption considerations and understand their implications on your organization.
   - Evaluate the impact of the considerations on your business solution and implementation.
   - Test Shield Platform Encryption in a sandbox environment before deploying to a production environment.
   - Before enabling encryption, fix any violations that you uncover. For example, referencing encrypted fields in a SOQL WHERE clause triggers a violation. Similarly, if you reference encrypted fields in a SOQL ORDER BY clause, a violation occurs. In both cases, fix the violation by removing references to the encrypted fields.

5. Analyze and test AppExchange apps before deploying them.
   - If you use an app from the AppExchange, test how it interacts with encrypted data in your organization and evaluate whether its functionality is affected.
   - If an app interacts with encrypted data that's stored outside of Salesforce, investigate how and where data processing occurs and how information is protected.
   - If you suspect Shield Platform Encryption could affect the functionality of an app, ask the provider for help with evaluation. Also discuss any custom solutions that must be compatible with Shield Platform Encryption.
   - Apps on the AppExchange that are built exclusively using Force.com inherit Shield Platform Encryption capabilities and limitations.

6. Platform Encryption is not a user authentication or authorization tool. Use field-level security settings, page layout settings, and validation rules, not Platform Encryption, to control which users can see which data.
7. Grant the “Manage Encryption Keys” user permission to authorized users only.

   Users with the “Manage Encryption Keys” permission can generate, export, import, and destroy organization-specific keys. Monitor the key management activities of these users regularly with the setup audit trail.

8. Mass-encrypt your existing data.

   Existing field and file data is not automatically encrypted when you turn on Shield Platform Encryption. To encrypt existing field data, update the records associated with the field data. This action triggers encryption for these records so that your existing data is encrypted at rest. To encrypt existing files, contact Salesforce.

9. Don't use Currency and Number fields for sensitive data.

   You can often keep private, sensitive, or regulated data safe without encrypting associated `Currency` or `Number` fields. Encrypting these fields could have broad functional consequences across the platform, such as disruptions to roll-up summary reports, report timeframes, and calculations, so they are not encryptable.

10. Communicate to your users about the impact of encryption.

    Before you enable Shield Platform Encryption in a production environment, inform users about how it affects your business solution. For example, share the information described in Shield Platform Encryption considerations, where it's relevant to your business processes.

11. Encrypt your data using the most current key.

    When you generate a new tenant secret, any new data is encrypted using this key. However, existing sensitive data remains encrypted using previous keys. In this situation, Salesforce strongly recommends re-encrypting these fields using the latest key. Contact Salesforce for help with this.

SEE ALSO:

- Back to Parent Topic
- https://resources.docs.salesforce.com/202/latest/en-us/sfdc/pdf/salesforce_platform_encryption_implementation_guide.pdf

Tradeoffs and Limitations of Shield Platform Encryption

A security solution as powerful as Shield Platform Encryption doesn't come without some tradeoffs. When your data is encrypted, some users may see limitations to some functionality, and a few features aren't available at all. Consider the impact on your users and your overall business solution as you design your encryption strategy.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

IN THIS SECTION:

General Shield Platform Encryption Considerations

These considerations apply to all data that you encrypt using Shield Platform Encryption.

Which Salesforce Apps Don't Support Shield Platform Encryption?

Some Salesforce features work as expected when you work with data that's encrypted with Shield Platform Encryption. Others don't.

Shield Platform Encryption and the Lightning Experience

Shield Platform Encryption works the same way in the Lightning Experience as it does in Salesforce Classic, with a few minor exceptions.

Field Limits with Shield Platform Encryption

Under certain conditions, encrypting a field can impose limits on the values that you store in that field. If you expect users to enter non-ASCII values, such as Chinese, Japanese, or Korean-encoded data, we recommend creating validation rules to enforce these limits.

SEE ALSO:

- Platform Encryption Overview
- Fix Compatibility Problems
- Platform Encryption Implementation Guide

General Shield Platform Encryption Considerations

These considerations apply to all data that you encrypt using Shield Platform Encryption.

Note: Beginning with Spring '17, Shield Platform Encryption no longer masks encrypted data in the presentation layer. This may affect some users' ability to work with encrypted data. If you have data you don't want specific users to see, revisit their field-level security settings on page 312, record access settings, and object permissions on page 315.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Leads

Lead and Case assignment rules, workflow rules, and validation rules work normally when Lead fields are encrypted. However, matching and de-duplication of records during lead import doesn't work, and Einstein lead scoring is not available.

Apex Lead Conversion works normally, but PL-SQL-based lead conversion is not supported.

In the Lightning Email Composer, the To: field is not autopopulated when the Name or Email field is encrypted.

Note: This beta version of encryption support in Leads is production quality but has known limitations.

Flows and Processes

You can reference encrypted fields in most places in your flows and processes. However, you can't reference encrypted fields in these filtering or sorting contexts.

Tool	Filtering Availability	Sorting Availability
Process Builder	Update Records action	n/a
Cloud Flow Designer	Dynamic Record Choice resource Fast Lookup element Record Delete element Record Lookup element Record Update element	Dynamic Record Choice resource Fast Lookup element Record Lookup element

You can store the value from an encrypted field in a variable and operate on that value in your flow's logic. You can also update the value for an encrypted field.

Paused flow interviews can result in data being saved in an unencrypted state. When a flow or process is waiting to resume, the associated flow interview is serialized and saved to the database. The flow interview is serialized and saved when:

- Users pause a flow
- Flows execute a Wait element
- Processes are waiting to execute scheduled actions

If the flow or process loads encrypted fields into a variable during these processes, that data might not be encrypted at rest.

Custom Fields

You can’t use encrypted custom fields in criteria-based sharing rules.

Some custom fields can’t be encrypted.

- Fields that have the `Unique` or `External ID` attributes or include these attributes on previously encrypted custom fields
- Fields on external data objects
- Fields that are used in an account contact relation

You can’t use Schema Builder to create an encrypted custom field.

SOQL/SOSL

- Encrypted fields can’t be used with the following SOQL and SOSL clauses and functions:
  - Aggregate functions such as MAX(), MIN(), and COUNT_DISTINCT()
  - WHERE clause
  - GROUP BY clause
  - ORDER BY clause

  Tip: Consider whether you can replace a WHERE clause in a SOQL query with a FIND query in SOSL.

- When you query encrypted data, invalid strings return an `INVALID_FIELD` error instead of the expected `MALFORMED_QUERY`.

Portals

If a portal is enabled in your organization, you can’t encrypt standard fields. Deactivate all customer portals and partner portals to enable encryption on standard fields. (Communities are supported.)

Search

If you encrypt fields with a key and then destroy the key, the corresponding search terms remain in the search index. However, you can’t decrypt the data associated with the destroyed key.

Accounts, Person Accounts, and Contacts

When Person Accounts are turned on, encrypting any of the following Account fields encrypts the equivalent Contact fields, and vice versa.

- Name
- Description
- Phone
- Fax

When you encrypt any of the following Account or Contact fields, the equivalent fields in Person Accounts are also encrypted.

- Name
- Description
- Mailing Address
- Phone
- Fax
- Mobile

- Home Phone
- Other Phone
- Email

When the Account Name or Contact Name field is encrypted, searching for duplicate accounts or contacts to merge doesn’t return any results.

When you encrypt the First Name or Last Name field on a contact, that contact appears in the Calendar Inviter lookup only if you haven’t filtered by First Name or Last Name.

Email

- When the standard Email field is encrypted, email to Salesforce can’t receive inbound emails.
- When the standard Email field is encrypted, the detail page for Contacts, Leads, or Person Accounts doesn’t flag invalid email addresses. If you need bounce processing to work as expected, don't encrypt the standard Email field.

Activities

Items in an Activity History related list may be displayed in plaintext even if the fields they refer to are encrypted.

Campaigns

Campaign member search isn’t supported when you search by encrypted fields.

Notes

You can encrypt the body text of Notes created with the new Notes tool. However, the Preview file and Notes created with the old Notes tool aren’t supported.

Field Audit Trail

Data in a previously archived Field Audit Trail isn’t encrypted when you turn on Platform Encryption. For example, say that your org uses Field Audit Trail to define a data history retention policy for an account field, such as the phone number field. When you turn on encryption for that field, new phone number records are encrypted as they are created. Previous updates to the phone number field that are stored in the Account History related list are also encrypted. However, phone number history data that is already archived in the `FieldHistoryArchive` object is stored without encryption. If you need to encrypt previously archived data, contact Salesforce.

Communities

If you encrypt the Account Name field and you’re not using Person Accounts, encryption affects how users’ roles are displayed to admins. Normally, a community user’s role name is displayed as a combination of their account name and the name of their user profile. When you encrypt the Account Name field, the account ID is displayed instead of the account name.

For example, when the Account Name field is not encrypted, users belonging to the Acme account with the Customer User profile would have a role called `Acme Customer User`. When Account Name is encrypted (and Person Accounts aren’t in use), the role is displayed as something like `001D000000IRt53 Customer User`.

REST API

You don’t get autosuggestions via the REST API when a field is encrypted.

Data Import

You can’t use the Data Import Wizard to perform matching using master-detail relationships or update records that contain encrypted fields. You can use it to add new records, however.

Reports, Dashboards, and List Views

- Report charts and dashboard components that display encrypted field values may be cached unencrypted.
- You can’t sort records in list views by fields that are encrypted.

Encryption for Chatter (Pilot)

When you embed a custom component in your Chatter feed using Rich Publisher Add-Ons (Pilot), the data related to those add-ons is encoded, but it isn’t encrypted with the Shield Platform Encryption service. Unencrypted data in Rich Publisher Add-Ons includes data stored in the Extension ID, Text Representation, Thumbnail URL, Title, Payload, and PayloadVersion fields.

General

- Encrypted fields can’t be used in:
  - Criteria-based sharing rules
  - Similar opportunities searches
  - External lookup relationships
  - Filter criteria for data management tools
  - Duplicate Management matching rules
- Live Agent chat transcripts are not encrypted at rest.
- Web-to-Case is supported, but the Web Company, Web Email, Web Name, and Web Phone fields are not encrypted at rest.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

SEE ALSO:

Back to Parent Topic

Which Salesforce Apps Don't Support Shield Platform Encryption?

Some Salesforce features work as expected when you work with data that's encrypted with Shield Platform Encryption. Others don't.

These apps don't support data encrypted with Shield Platform Encryption. However, you can enable Shield Platform Encryption for other apps when these apps are in use.

- Connect Offline
- Commerce Cloud
- Data.com
- Heroku (but Heroku Connect does support encrypted data)
- Marketing Cloud (but Marketing Cloud Connect does support encrypted data)
- Pardot (but Pardot Connect supports encrypted contact email addresses if your Pardot org allows multiple prospects with the same email address)
- Salesforce Mobile Classic
- Salesforce IQ
- Social Customer Service
- Steelbrick
- Thunder
- Quip

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Legacy portals (customer, self-service, and partner) don't support data encrypted with Shield Platform Encryption. If legacy portals are active, Shield Platform Encryption can't be enabled.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

SEE ALSO:

Back to Parent Topic

Shield Platform Encryption and the Lightning Experience

Shield Platform Encryption works the same way in the Lightning Experience as it does in Salesforce Classic, with a few minor exceptions.

Contacts and Leads

In Lightning, if either the **Name** or **Email** field is encrypted, Salesforce doesn't suggest email recipients from contacts you've emailed before."

Notes

Note previews in Lightning are not encrypted.

File Encryption Icon

The icon that indicates that a file is encrypted doesn't appear in Lightning.

Date Fields

Lightning shows 12/30/0001 as the dummy date for masking encrypted date values.

Custom Field Masking

When the encryption key is destroyed, the values of encrypted custom field values may appear in plaintext until the page is refreshed.

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Field Limits with Shield Platform Encryption

Under certain conditions, encrypting a field can impose limits on the values that you store in that field. If you expect users to enter non-ASCII values, such as Chinese, Japanese, or Korean-encoded data, we recommend creating validation rules to enforce these limits.

	API Length	Byte Length	Non-ASCII characters
Assistant Name	40	120	22
City	40	120	22
Company (Lead)	255	765	No limitation
Description (Case, Account, Contact, Lead)	32000	96000	No limitation
Email	80	240	70
Fax	40	120	22
First Name	40	120	22
Last Name	80	240	70
Middle Name	40	120	22
Next Step (Opportunity)	128	384	126
Phone	40	120	22
Street	255	765	No limitation
Subject (Case)	255	765	No limitation
Title	128	384	126

EDITIONS

Available as an add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Requires purchasing Salesforce Shield. Available in **Developer** Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

Note: This is not an exhaustive list. For information about a field not shown here, refer to the API.

Case Comment Object

The Body field on the Case Comment object has a limit of 4,000 ASCII characters (or 4,000 bytes). However, when these fields are encrypted, the character limit is lower. How much lower depends on the kind of characters you enter.

- ASCII: 2959
- Chinese, Japanese, Korean: 1333
- Other non-ASCII: 1479

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

SEE ALSO:

Encrypt New Data in Fields

Back to Parent Topic

Session Security

After logging in, a user establishes a session with the platform. Use session security to limit exposure to your network when a user leaves the computer unattended while still logged in. Session security also limits the risk of internal attacks, such as when one employee tries to use another employee's session. Choose from several session settings to control session behavior.

You can control when an inactive user session expires. The default session timeout is two hours of inactivity. When the session timeout is reached, users are prompted with a dialog that allows them to log out or continue working. If they don't respond to this prompt, they are logged out.

Note: When users close a browser window or tab, they aren't automatically logged out from their Salesforce session. Ensure that your users are aware of this behavior and that they end all sessions properly by selecting *Your Name* > **Logout**.

By default, Salesforce uses TLS (Transport Layer Security) and requires secure connections (HTTPS) for all communication. The `Require secure connections (HTTPS)` setting determines whether TLS (HTTPS) is required for access to Salesforce. If you ask Salesforce to disable this setting and change the URL from `https://` to `http://`, you can still access the application. However, for added security, require all sessions to use TLS. For more information, see Modify Session Security Settings on page 585.

You can restrict access to certain types of resources based on the level of security associated with the authentication (login) method for the user's current session. By default, each login method has one of two security levels: Standard or High Assurance. You can change the session security level and define policies so specified resources are only available to users with a High Assurance level. For details, see Session-level Security on page 590.

You can control whether your org stores user logins and whether they can appear from the Switcher with the settings **Enable caching and autocomplete on login page**, **Enable user switching**, and **Remember me until logout**.

IN THIS SECTION:

Modify Session Security Settings

You can modify session security settings to specify session connection type, timeout settings, and IP address ranges to protect against malicious attacks and more.

Enable Browser Security Settings

Browser security settings protect sensitive information and monitor SSL certificates.

Set Trusted IP Ranges for Your Organization

Trusted IP Ranges define a list of IP addresses from which users can log in without receiving a login challenge for verification of their identity, such as a code sent to their mobile phone.

User Sessions

Monitor and protect your Salesforce org by reviewing active sessions and session details on the User Session Information page. You can create custom list views, view details about a user associated with a specific session, and easily end suspicious sessions. Salesforce admins can view all user sessions for an org; non-admins see only their own sessions.

Understanding Session Types

Learn about the session types in the User Session Information page to help you monitor and protect your organization.

SEE ALSO:

Set Trusted IP Ranges for Your Organization

Identity Verification History

Modify Session Security Settings

You can modify session security settings to specify session connection type, timeout settings, and IP address ranges to protect against malicious attacks and more.

1. From Setup, enter `Session Settings` in the Quick Find box, then select **Session Settings**.
2. Customize the session security settings.

Field	Description
`Timeout value`	Length of time after which the system logs out inactive users. For Portal users, the timeout is between 10 minutes and 24 hours even though you can only set it as low as 15 minutes. Select a value between 15 minutes and 24 hours. Choose a shorter timeout period if your org has sensitive information and you want to enforce stricter security. Note: The last active session time value isn't updated until halfway through the timeout period. So if you have a 30-minute timeout, the system doesn't check for activity until 15 minutes have passed. For example, if you update a record after 10 minutes, the last active session time value isn't updated because there was no activity after 15 minutes. You're logged out in 20 more minutes (30 minutes total), because the last active session time wasn't updated. Suppose that you update a record after 20 minutes. That's 5 minutes after the last active session time is checked. Your timeout resets, and you have another 30 minutes before being logged out, for a total of 50 minutes.
`Disable session timeout warning popup`	Determines whether the system prompts inactive users with a timeout warning message. Users are prompted 30 seconds before timeout as specified by the `Timeout value`.
`Force logout on session timeout`	Requires that when sessions time out for inactive users, current sessions become invalid. The browser refreshes and returns to the login page. To access the org, the user must log in again. Note: Do *not* select `Disable session timeout warning popup` when using this setting.
`Lock sessions to the IP address from which they originated`	Determines whether user sessions are locked to the IP address from which the user logged in, helping to prevent unauthorized persons from hijacking a valid session.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

The `Lock sessions to the IP address from which they originated` setting is available in: **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

All other settings available in: **Essentials**, **Personal**, **Contact Manager**, **Group**, **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

USER PERMISSIONS

To modify session security settings:

- Customize Application

Field	Description
	Note: This setting can inhibit various applications and mobile devices.
Lock sessions to the domain in which they were first used	Associates a current UI session for a user, such as a community user, with a specific domain. The setting helps prevent unauthorized use of the session ID in another domain. This setting is enabled by default for orgs created with the Spring '15 release or later.
Require secure connections (HTTPS)	Determines whether HTTPS is required to log in to or access Salesforce. This setting is enabled by default for security reasons. This setting does not apply to API requests. All API requests require HTTPS. To enable HTTPS on communities and Force.com sites see: HSTS for Sites and Communities Note: The Reset Passwords for Your Users page can only be accessed using HTTPS.
Require secure connections (HTTPS) for all third-party domains	Determines whether HTTPS is required for connecting to third-party domains. This setting is enabled by default on accounts created after the Summer '17 release.
Force relogin after Login-As-User	Determines whether an administrator who is logged in as another user is returned to their previous session after logging out as the secondary user. If the setting is enabled, an administrator must log in again to continue using Salesforce after logging out as the user. Otherwise, the administrator is returned to the original session after logging out as the user. This setting is enabled by default for new orgs beginning with the Summer '14 release.
Require HttpOnly attribute	Restricts session ID cookie access. A cookie with the HttpOnly attribute is not accessible via non-HTTP methods, such as calls from JavaScript. Note: If you have a custom or packaged application that uses JavaScript to access session ID cookies, selecting Require HttpOnly attribute breaks your application. It denies the application access to the cookie. If Require HttpOnly attribute is selected, the AJAX Toolkit debugging window isn't available.

Use POST requests for cross-domain sessions	Sets the org to send session information using a POST request, instead of a GET request, for cross-domain exchanges. An example of a cross-domain exchange is when a user is using a Visualforce page. In this context, POST requests are more secure than GET requests because POST requests keep the session information in the body of the request. However, if you enable this setting, embedded content from another domain, such as:
	`<img`
	`src="https://acme.force.com/pic.jpg"/>`

Field	Description
	sometimes doesn't display.
`Enforce login IP ranges on every request`	Restricts the IP addresses from which users can access Salesforce to only the IP addresses defined in `Login IP Ranges`. If this setting is enabled, login IP ranges are enforced on each page request, including requests from client applications. If this setting isn't enabled, login IP ranges are enforced only when a user logs in. This setting affects all user profiles that have login IP restrictions.
`Enable caching and autocomplete on login page`	Allows the user's browser to store usernames. If enabled, after initial login, usernames are auto-filled into the `Username` field on the login page. If the user selected **Remember me** on the login page, the username persists after the session expires or the user logs out. The username also appears on the Switcher. This setting is selected by default for all orgs. Note: If you disable this setting, the **Remember me** option doesn't appear on your org's login page or from the Switcher.
`Enable secure and persistent browser caching to improve performance`	Enables secure data caching in the browser to improve page reload performance by avoiding extra round trips to the server. This setting is selected by default for all orgs. We don't recommend disabling this setting, but if your company's policy doesn't allow browser caching even if the data is encrypted, you can disable it.
`Enable user switching`	Determines whether the Switcher appears when your org's users select their profile picture. This setting is selected by default for all organizations. The `Enable caching and autocomplete on login page` setting must also be enabled. Deselect the `Enable user switching` setting to prevent your org from appearing in Switchers on other orgs. It also prevents your org users from seeing the Switcher when they select their profile picture.
`Remember until logout`	Normally, usernames are cached only while a session is active or if a user selects **Remember Me**. For SSO sessions, the remember option isn't available. So, once the session expires, the username disappears from the login page and the Switcher. By enabling `Remember me until logout`, the cached usernames are deleted only if the user explicitly logs out. If the session times out, they appear on the Switcher as inactive. This way, if the users are on their own computer and allow a session to timeout, they can select the username to reauthenticate. If they're on a shared computer, the username is deleted immediately when the user logs out. This setting applies to all your org's users. This option isn't enabled by default. However, we encourage you to enable it as a convenience to your users. Keep this setting disabled if your org doesn't expose all your SSO or authentication providers on your login page.
`Enable the SMS method of identity confirmation`	Allows users to receive a one-time PIN delivered via SMS. If this setting is selected, administrators or users must verify their mobile phone number before taking advantage of this feature. This setting is selected by default for all orgs.

Field	Description
`Require security tokens for API logins from callouts (API version 31.0 and earlier)`	In API version 31.0 and earlier, requires the use of security tokens for API logins from callouts. Examples are Apex callouts or callouts using the AJAX proxy. In API version 32.0 and later, security tokens are required by default.
`Login IP Ranges` (for Contact Manager, Group, and Professional Editions)	Specifies a range of IP addresses users must log in from (inclusive), or the login fails. To specify a range, click **New** and enter a Start IP Address and End IP Address to define the range, which includes the start and end values. This field is not available in Enterprise, Unlimited, Performance, and Developer Editions. In those editions, you can specify a valid Login IP Range in the user profile settings.
`Let users use a security key (U2F)`	Allows users to use a U2F security key for two-factor authentication and identity verification. Instead of using Salesforce Authenticator, a one-time password generated by an authenticator app, or one-time passwords sent by email or SMS, users insert their registered U2F security key into a USB port to complete verification.
`Require identity verification during two-factor authentication registration`	Requires users to confirm their identities to add a two-factor authentication method, such as Salesforce Authenticator, instead of requiring a relogin as before.
`Require identity verification for change of email address`	Requires users to confirm their identities to change email addresses instead of requiring a relogin as before. Note: To get the emails to confirm identity, make sure that users have access to their previously registered email accounts.

`Allow location-based automated verifications with Salesforce Authenticator`
`Allow only from trusted IP addresses`
	Allows users to verify identity by automatically approving notifications in Salesforce Authenticator, whenever users are in trusted locations such as a home or office. If you allow automated verifications, you can allow them from any location or restrict them to only trusted IP addresses, such as your corporate network.

`Allow Lightning Login`	Allows users to use Lightning Login for password-free Salesforce logins, relying on Salesforce Authenticator for identity verification.
`Enable clickjack protection for Setup pages`	Protects against clickjack attacks on setup Salesforce pages. Clickjacking is also known as a user interface redress attack. (Setup pages are available from the Setup menu.)
`Enable clickjack protection for non-Setup Salesforce pages`	Protects against clickjack attacks on non-setup Salesforce pages. Clickjacking is also known as a user interface redress attack. Setup pages already include protection against clickjack attacks. (Setup pages are available from the Setup menu.) This setting is selected by default for all orgs.

Field	Description
`Enable clickjack protection for customer Visualforce pages with standard headers`	Protects against clickjack attacks on your Visualforce pages with headers enabled. Clickjacking is also known as a user interface redress attack. Warning: If you use custom Visualforce pages within a frame or iframe, you sometimes see a blank page or the page displays without the frame. For example, Visualforce pages in a page layout don't function when clickjack protection is on.
`Enable clickjack protection for customer Visualforce pages with headers disabled`	Protects against clickjack attacks on your Visualforce pages with headers disabled when setting `showHeader="false"` on the page. Clickjacking is also known as a user interface redress attack. Warning: If you use custom Visualforce pages within a frame or iframe, you sometimes see a blank page or the page displays without the frame. For example, Visualforce pages in a page layout don't function when clickjack protection is on.
`Enable CSRF protection on GET requests on non-setup pages`	Protects against Cross Site Request Forgery (CSRF) attacks by modifying non-Setup pages. Non-Setup pages include a random string of characters in the URL parameters or as a hidden form field. With every GET and POST request, the application checks the validity of this string of characters. The application doesn't execute the command unless the value found matches the expected value. This setting is selected by default for all orgs.
`Enable CSRF protection on POST requests on non-setup pages`	
`XSS protection`	Protects against reflected cross-site scripting attacks. If a reflected cross-site scripting attack is detected, the browser shows a blank page with no content.
`Content Sniffing protection`	Prevents the browser from inferring the MIME type from the document content. It also prevents the browser from executing malicious files (JavaScript, Stylesheet) as dynamic content.
`Referrer URL Protection`	When loading pages, the referrer header shows only Salesforce.com rather than the entire URL. This feature eliminates the potential for a referrer header to reveal sensitive information that could be present in a full URL, such as an org ID. This feature is supported only for Chrome and Firefox.
`HSTS for Sites and Communities`	Requires HTTPS on communities and Force.com sites. Note: This setting must be enabled in two locations. `HSTS for Sites and Communities` must be enabled in Session Settings, and `Require Secure Connections (HTTPS)` must be enabled in the community or Force.com site security settings. See Creating and Editing Force.com Sites.
`Logout URL`	Redirects users to a specific page after they log out of Salesforce, such as an authentication provider's page or a custom-branded page. This URL is used only if no logout URL is specified in the identity provider, SAML single sign-on, or external authentication provider settings. If no value is specified for `Logout URL`, the default is `https://login.salesforce.com`, unless

Field	Description
	MyDomain is enabled. If My Domain is enabled, the default is `https://customdomain.my.salesforce.com`.

3. Click **Save**.

Session Security Levels

You can restrict access to certain types of resources based on the level of security associated with the authentication (login) method for the user's current session. By default, each login method has one of two security levels: Standard or High Assurance. You can change the session security level and define policies so specified resources are only available to users with a High Assurance level.

The different authentication methods are assigned these security levels, by default.

- Username and Password — Standard
- Delegated Authentication — Standard
- Activation — Standard
- Lightning Login — Standard
- Two-Factor Authentication — High Assurance
- Authentication Provider — Standard
- SAML — Standard

> Note: The security level for a SAML session can also be specified using the `SessionLevel` attribute of the SAML assertion sent by the identity provider. The attribute can take one of two values, `STANDARD` or `HIGH_ASSURANCE`.

To change the security level associated with a login method:

1. From Setup, enter *`Session Settings`* in the `Quick Find` box, then select **Session Settings**.
2. Under Session Security Levels, select the login method.
3. To move the method to the proper category, click the **Add** or **Remove** arrow.

Currently, the only features that use session-level security are reports and dashboards in Salesforce and connected apps. You can set policies requiring High Assurance on these types of resources. You can also specify an action to take if the session used to access the resource is not High Assurance. The supported actions are:

- Block — Blocks access to the resource by showing an insufficient privileges error.
- Raise session level — Prompts users to complete two-factor authentication. When users authenticate successfully, they can access the resource. For reports and dashboards, you can apply this action when users access reports or dashboards, or just when they export and print them.

> Warning: Raising the session level to high assurance by redirecting the user to complete two-factor authentication is not a supported action in Lightning Experience. If your org has Lightning Experience enabled, and you set a policy that requires a high assurance session to access reports and dashboards, Lightning Experience users with a standard assurance session are blocked from reports and dashboards. Also, they don't see the icons for these resources in the navigation menu. As a workaround, users with a standard assurance session can log out and log in again using an authentication method that is defined as high assurance by their org. Then they have access to reports and dashboards. Or, they can switch to Salesforce Classic, where they're prompted to raise the session level when they attempt to access reports and dashboards.

To set a High Assurance required policy for accessing a connected app:

1. From Setup, enter `Connected Apps` in the `Quick Find` box, then select the option for managing connected apps.
2. Click **Edit** next to the connected app.
3. Select **High Assurance session required**.
4. Select one of the actions presented.
5. Click **Save**.

To set a High Assurance required policy for accessing reports and dashboards:

1. From Setup, enter `Access Policies` in the `Quick Find` box, then select **Access Policies**.
2. Select **High Assurance session required**.
3. Select one of the actions presented.
4. Click **Save**.

Session levels have no impact on resources in the app other than connected apps, reports, and dashboards for which explicit security policies have been defined.

SEE ALSO:

Session Security

Explore the Salesforce Setup Menu

Identity Verification History

Enable Browser Security Settings

Browser security settings protect sensitive information and monitor SSL certificates.

Referrer URL Protection

When loading assets outside of Salesforce or navigating outside of Salesforce, the referrer header shows only Salesforce.com or Force.com rather than the entire URL. This feature eliminates the potential for a referrer header to reveal sensitive information that could be present in a full URL, such as an org ID. This feature is supported only for Chrome and Firefox.

Public Key Pinning

To detect man-in-the-middle attacks, Salesforce now monitors which SSL certificates users can see. Custom certificates aren't affected. Public key pinning is supported only for Chrome and Firefox.

HSTS (HTTP Strict Transport Security) Protection

HSTS redirects browsers to use HTTPS. It is enabled on all Salesforce and Visualforce pages, and it can't be disabled. You can choose to enable HSTS on communities and Force.com sites. When you enable HSTS on a subdomain, it's also applied to the communities or Force.com sites that share the subdomain.

After HSTS is enabled, the browser caches that only HTTPS can be used on the domain. The cache is saved for one year.

Enabling HSTS

Lightning Communities

1. From Setup, enter `Session Settings` in the Quick Find box, then select **Session Settings**.
2. Select **HSTS for Sites and Communities**, and click **Save**.
3. On the Site.com tab in the Site.com app, launch Site.com Studio.

4. Select **Site Configuration**, and then select **Require Secure Connections (HTTPS)**, and click **Save**.

Force.com Sites

1. From Setup, enter `Session Settings` in the Quick Find box, then select **Session Settings**.
2. Select **HSTS for Sites and Communities**, and click **Save**.
3. From Setup, enter `Sites` in the Quick Find box, then select **Sites**.
4. On the Force.com site, select **Edit**, and then select **Require Secure Connections (HTTPS)**, and click **Save**.

Communities and Force.com Sites Using a Custom Domain

1. From Setup, enter `Session Settings` in the Quick Find box, then select **Session Settings**.
2. Select **HSTS for Sites and Communities**, and click **Save**.
3. For a Lightning community custom domain:

   a. On the Site.com tab in the Site.com app, launch Site.com Studio.

   b. Select **Site Configuration**, and then select **Require Secure Connections (HTTPS)**, and click **Save**.

4. For a Force.com site custom domain:

   a. From Setup, enter `Sites` in the Quick Find box, then select **Sites**.

   b. Click **Edit** on the Force.com site and select **Require Secure Connections (HTTPS)** and **Save**.

5. From Setup, enter `Domains` in the Quick Find box, then select **Domains**.
6. On the domain, click **Edit**. Select **Enable Strict Transport Security headers**, and click **Save**.

Set Trusted IP Ranges for Your Organization

Trusted IP Ranges define a list of IP addresses from which users can log in without receiving a login challenge for verification of their identity, such as a code sent to their mobile phone.

Note: Who Sees What: Organization Access (English only)

Watch how you can restrict login through IP ranges and login hours.

To help protect your organization's data from unauthorized access, you can specify a list of IP addresses from which users can log in without receiving a login challenge. However, this does not restrict access, entirely, for users outside of the Trusted IP Range. After these users complete the login challenge (usually by entering a code sent to their mobile device or email address), they can log in.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To change network access:
- Manage IP Addresses

1. From Setup, enter `Network Access` in the `Quick Find` box, then select **Network Access**.
2. Click **New**.
3. Enter a valid IP address in the `Start IP Address` field and a higher IP address in the `End IP Address` field.

   The start and end addresses define the range of allowable IP addresses from which users can log in, including the start and end values. If you want to allow logins from a single IP address, enter the same address in both fields.

   The start and end IP addresses must be in an IPv4 range and include no more than 33,554,432 addresses (2^{25}, a /7 CIDR block).

4. Optionally, enter a description for the range. For example, if you maintain multiple ranges, enter details about the part of your network that corresponds to this range.

5. Click **Save**.

Note: For organizations that were activated before December 2007, Salesforce automatically populated your organization's trusted IP address list in December 2007, when this feature was introduced. The IP addresses from which trusted users had already accessed Salesforce during the past six months were added.

SEE ALSO:

Session Security

Restrict Where and When Users Can Log In to Salesforce

Security Implementation Guide

User Sessions

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

Monitor and protect your Salesforce org by reviewing active sessions and session details on the User Session Information page. You can create custom list views, view details about a user associated with a specific session, and easily end suspicious sessions. Salesforce admins can view all user sessions for an org; non-admins see only their own sessions.

When you manually end a user's session by clicking the **Remove** button, the user must log in again to the organization.

The following table contains information about the fields you can view on this page. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) may vary.

Field	Description
City	The city where the user's IP address is physically located. This value is not localized.
Country	The country where the user's IP address is physically located. This value is not localized.
Country Code	The ISO 3166 code for the country where the user's IP address is physically located. This value is not localized. For more information, see Country Codes - ISO 3166.
Created	The date and time stamp of when the session began.
Latitude	The latitude where the user's IP address is physically located.
Location	The approximate location of the IP address from where the user logged in. To show more geographic information, such as approximate city and postal code, create a custom view to include those fields. This value is not localized.
Longitude	The longitude where the user's IP address is physically located.
Login Type	The type of login associated with the session. Some login types include Application, SAML, and Portal.
Parent Session ID	If a session has a parent, this ID is the parent's unique ID.
Postal Code	The postal code where the user's IP address is physically located. This value is not localized.
Session ID	The unique ID for the session.
Session Type	The type of session the user is logged in to. For example, common ones are UI, Content, API, and Visualforce.

Field	Description
Source IP	The IP address associated with the session.
Subdivision	The name of the subdivision where the user's IP address is physically located. This value is not localized.
User Type	The profile type associated with the session.
Username	The username used when logged in to the session. To view the user's profile page, click the username.
Updated	The date and time stamp of the last session update due to activity. For example, during a UI session, users make frequent changes to records and other data as they work. With each change, both the `Updated` and `Valid Until` date and time stamps are refreshed.
Valid Until	If you don't end the session manually, the date and time stamp of when the session automatically expires.

SEE ALSO:

The Elements of User Authentication

Understanding Session Types

Understanding Session Types

Learn about the session types in the User Session Information page to help you monitor and protect your organization.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

You can view the session type for a specific user on the User Session Information page. To access the page from Setup, enter *Session Management* in the `Quick Find` box, then select **Session Management**.

Session types indicate the type of session a user is utilizing to access an organization. Session types can be persistent or temporary and accessed via the user interface, API, or other methods, such as an OAuth authentication process.

The following table describes the session types.

Session Type	Description
API	Created when accessing an organization through the API.
APIOnlyUser	Created to enable a password reset in the user interface for API-only users.
Chatter Networks	Created when using Chatter Networks or Chatter Communities.
ChatterNetworksAPIOnly	Created when using the Chatter Networks or Chatter Communities API.
Content	Created when serving user-uploaded content.
OauthApprovalUI	A session that only allows access to the OAuth approval page.
Oauth2	Created via OAuth flows. For example, if you use OAuth authentication for a connected app, this type of session is created.
SiteStudio	Created when using the Sites Studio user interface.

Session Type	Description
SitePreview	A session that is initiated when an internal canvas app is invoked. This will always be a child session with a UI parent session.
SubstituteUser	A session created when one user logs in via another user. For example, if an administrator logs in as another user, a SubstituteUser session is created.
TempContentExchange	A temporary user interface session to switch to the content domain, such as the user interface into which users type in their credentials.
TempOauthAccessTokenFrontdoor	A temporary session via the OAuth access token assertion flow that cannot be refreshed and must be mapped to a regular session type.
TempVisualforceExchange	A temporary session to switch to the Visualforce domain.
TempUIFrontdoor	A temporary session that cannot be refreshed and must be mapped to a regular session type.
UI	Created when using a user interface page.
UserSite	Initiated when a canvas application is invoked. Always a child session with a UI parent session.
Visualforce	Created via a Visualforce page.
WDC_API	A session using the Work.com API. This is always a child session and cannot be used in the user interface.

SEE ALSO:

The Elements of User Authentication

User Sessions

Activations

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

Available in all editions

Activation tracks information about devices from which users have verified their identity. Salesforce prompts users to verify their identity when they access Salesforce from an unrecognized browser or application. Identity verification adds an extra layer of security on top of username and password authentication. The Activations page lists the login IP addresses and client browsers used.

When a user logs in from outside a trusted IP range and uses a browser or app we don't recognize, the user is challenged to verify identity. We use the highest-priority verification method available for each user. In order of priority, the methods are:

1. Verification via push notification or location-based automated verification with the Salesforce Authenticator mobile app (version 2 or later) connected to the user's account.
2. Verification via a U2F security key registered with the user's account.
3. Verification code generated by a mobile authenticator app connected to the user's account.
4. Verification code sent via SMS to the user's verified mobile phone.
5. Verification code sent via email to the user's email address.

After identity verification is successful, the user doesn't have to verify identity again from that browser or app, unless the user:

- Manually clears browser cookies, sets the browser to delete cookies, or browses in private or incognito mode
- Deselects **Don't ask again** on the identity verification page

The Activations page in Setup lists the login IP addresses and client browser information of devices from which users have verified their identity. You can revoke the browser activation status for one, many, or all users.

For example, a user reports a lost device and is issued a new one. You can revoke the activation status of the browser on the lost device so that anyone attempting to access the org from that device has to verify their identity. This identity verification adds a layer of security while allowing users to stay productive.

Users can view their own Activations page to check their login IP addresses and client browser information. End users can revoke the activation status only for their own activated browsers.

For example, a user logs in to the org. On the user's Activations page, several different browsers are activated, but the user has only logged in from a single browser on a work laptop. The user immediately revokes the activation status of those browsers the user doesn't recognize. Because this user is challenged for identity verification using a code sent via SMS to the user's mobile device, anyone else who tries to log in from one of the deactivated browsers can't get the texted verification code. Without the code, the hacker fails the identity verification challenge. The user can then report the potential security breach.

IN THIS SECTION:

Use Activations

View your users' activations and revoke activation status to prevent security breaches.

SEE ALSO:

Use Activations

Identity Verification History

Use Activations

View your users' activations and revoke activation status to prevent security breaches.

To see login IP and browser information about devices from which users have verified their identity, from Setup, enter `Activations` in the `Quick Find` box, then select **Activations**.

You can revoke activation status by selecting one or more entries in the Activated Client Browser list, clicking **Remove**, and confirming the action. Users can view and revoke only their own activated browsers. A user who logs in from a deactivated browser is prompted to verify identity, unless the login IP address is within a trusted IP range.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

Available in all editions

Note: When a user deselects the **Don't ask again** option that appears on the identity verification page, the browser isn't activated. Advise your users to deselect this option whenever they log in from a public or shared device.

SEE ALSO:

Activations

Identity Verification History

Authenticate Users

Authentication means preventing unauthorized access to your organization or its data by making sure each logged in user is who they say they are.

IN THIS SECTION:

The Elements of User Authentication

Salesforce provides a variety of ways to authenticate users. Build a combination of authentication methods that fits the needs of your organization and your users' use patterns.

Configure User Authentication

Choose login settings to ensure that your users are who they say they are.

The Elements of User Authentication

Salesforce provides a variety of ways to authenticate users. Build a combination of authentication methods that fits the needs of your organization and your users' use patterns.

IN THIS SECTION:

Single Sign-On

Salesforce has its own system of user authentication, but some companies prefer to use an existing single sign-on capability to simplify and standardize their user authentication.

Network-Based Security

Network-based security limits where users can log in from, and when they can log in. This is different from user authentication, which only determines who can log in. Use network-based security to limit the window of opportunity for an attacker and to make it more difficult for an attacker to use stolen credentials.

CAPTCHA Security for Data Exports

By request, Salesforce can require users to pass a simple text-entry user verification test to export data from Salesforce. This type of network-based security helps prevent malicious users from accessing your organization’s data, and can reduce the risk of automated attacks.

Restrict Where and When Users Can Log In to Salesforce

You can restrict the hours during which users can log in and the range of IP addresses from which they can log in and access Salesforce. If IP address restrictions are defined for a user’s profile and a login originates from an unknown IP address, Salesforce does not allow the login. These restrictions help protect your data from unauthorized access and phishing attacks.

Two-Factor Authentication

As a Salesforce admin, you can enhance your org’s security by requiring a second level of authentication for every user login. You can also require two-factor authentication when a user meets certain criteria, such as attempting to view reports or access a connected app.

Custom Login Flows

You can use a login flow to introduce business processes during login, such as to prompt for a second factor of authentication, accept terms of services, or collect information from users. After users complete the login flow, they’re logged in to Salesforce.

SEE ALSO:

Single Sign-On

Network-Based Security

CAPTCHA Security for Data Exports

User Sessions

Single Sign-On

Salesforce has its own system of user authentication, but some companies prefer to use an existing single sign-on capability to simplify and standardize their user authentication.

You have two options to implement single sign-on—federated authentication using Security Assertion Markup Language (SAML) or delegated authentication.

- Federated authentication using Security Assertion Markup Language (SAML) lets you send authentication and authorization data between affiliated but unrelated web services. You can log in to Salesforce from a client app. Salesforce enables federated authentication for your org automatically.
- Delegated authentication SSO integrates Salesforce with an authentication method that you choose. You can integrate authentication with your LDAP (Lightweight Directory Access Protocol) server or use a token instead of a password for authentication. You manage delegated authentication at the permission level, not at the org level, giving you more flexibility. With permissions, you can require some to use delegated authentication while others use their Salesforce-managed password.

  Delegated authentication offers the following benefits.

  - Uses a stronger form of user authentication, such as integration with a secure identity provider
  - Makes your login page private and accessible only behind a corporate firewall
  - Differentiates your org from all other companies that use Salesforce to reduce phishing attacks

  You must contact Salesforce to enable delegated authentication before you can configure it on your org.
- Authentication providers let your users log in to your Salesforce org using their login credentials from an external service provider. Salesforce supports the OpenID Connect protocol, which lets users log in from any OpenID Connect provider, such as Google, PayPal, and LinkedIn. When an authentication provider is enabled, Salesforce doesn't validate a user's password. Instead, Salesforce uses the user's login credentials from the external service provider to establish authentication credentials.

Identity Providers

An *identity provider* is a trusted provider that lets you use single sign-on (SSO) to access other websites. A *service provider* is a website that hosts apps. You can enable Salesforce as an identity provider and define one or more service providers. Your users can then access other apps directly from Salesforce using SSO. SSO can be a great help to your users—instead of having to remember many passwords, they only have to remember one.

For more information, see "Identity Providers and Service Providers" in the Salesforce online help.

SEE ALSO:

The Elements of User Authentication

Network-Based Security

Network-based security limits where users can log in from, and when they can log in. This is different from user authentication, which only determines who can log in. Use network-based security to limit the window of opportunity for an attacker and to make it more difficult for an attacker to use stolen credentials.

SEE ALSO:

The Elements of User Authentication

CAPTCHA Security for Data Exports

By request, Salesforce can require users to pass a simple text-entry user verification test to export data from Salesforce. This type of network-based security helps prevent malicious users from accessing your organization's data, and can reduce the risk of automated attacks.

To pass the test, users must type two words displayed on an overlay into the overlay's text box field, and click a **Submit** button. Salesforce uses CAPTCHA technology provided by reCaptcha to verify that a person, as opposed to an automated program, has correctly entered the text into the overlay. CAPTCHA stands for "Completely Automated Public Turing test to tell Computers and Humans Apart."

SEE ALSO:

The Elements of User Authentication

Restrict Where and When Users Can Log In to Salesforce

You can restrict the hours during which users can log in and the range of IP addresses from which they can log in and access Salesforce. If IP address restrictions are defined for a user's profile and a login originates from an unknown IP address, Salesforce does not allow the login. These restrictions help protect your data from unauthorized access and phishing attacks.

Login Hours

For each profile, you can set the hours when users can log in. See:

- View and Edit Login Hours in the Enhanced Profile User Interface
- View and Edit Login Hours in the Original Profile User Interface

Two-Factor Authentication for User Interface Logins

For each profile, you can require users to use a second form of authentication when they log in via the user interface. See Set Two-Factor Authentication Login Requirements on page 600 and Set Two-Factor Authentication Login Requirements and Custom Policies for Single Sign-On, Social Sign-On, and Communities.

Two-Factor Authentication for API Logins

For each profile, you can require a verification code (also called a time-based one-time password, or TOTP) instead of the standard security token. Users connect an authenticator app that generates verification codes to their account. Users with the "Two-Factor Authentication for API Logins" permission use a code instead of the standard security token whenever it's requested, such as when resetting the account's password. See Set Two-Factor Authentication Login Requirements for API Access on page 603.

Login IP Address Ranges

For Enterprise, Performance, Unlimited, Developer, and Database.com editions, you can set the Login IP Range addresses from which users can log in on an individual profile. Users outside of the Login IP Range set on a profile can't access your Salesforce org.

For Contact Manager, Group, and Professional Editions, set the Login IP Range. From Setup, enter *Session Settings* in the `Quick Find` box, then select **Session Settings**.

Login IP Address Range Enforcement for All Access Requests

You can restrict all access to Salesforce to the IP addresses included in Login IP Ranges in users' profiles. For example, suppose a user logs in successfully from an IP address defined in Login IP Ranges. The user then moves to a different location and has a new IP address that is outside of Login IP Ranges. When the user refreshes the browser or tries to access Salesforce, including access from a client application, the user is denied. To enable this option, from Setup, enter `Session Settings` in the `Quick Find` box, select **Session Settings**, and then select **Enforce login IP ranges on every request**. This option affects all user profiles that have login IP restrictions.

Org-wide Trusted IP Ranges

For all users, you can set a list of IP address ranges from which they can always log in without receiving a login challenge. These users can log in to your org after they provide the additional verification. See Set Trusted IP Ranges for Your Organization.

When users log in to Salesforce via the user interface, the API, or a desktop client such as Salesforce for Outlook, Connect Offline, Connect for Office, or the Data Loader, Salesforce confirms that the login is authorized as follows.

1. Salesforce checks whether the user's profile has login hour restrictions. If login hour restrictions are specified for the user's profile, any login outside the specified hours is denied.
2. If the user has the "Two-Factor Authentication for User Interface Logins" permission, Salesforce prompts the user for a second form of authentication upon logging in. If the user's account isn't already connected to a mobile authenticator app such as Salesforce Authenticator, Salesforce first prompts the user to connect the app.
3. If the user has the "Two-Factor Authentication for API Logins" permission and has connected an authenticator app to the account, Salesforce returns an error if the user uses the standard security token. The user has to enter a verification code (time-based one-time password) generated by the authenticator app instead.
4. Salesforce then checks whether the user's profile has IP address restrictions. If IP address restrictions are defined for the user's profile, logins from an undesignated IP address are denied, and logins from a specified IP address are allowed. If the **Enforce login IP ranges on every request** session setting is enabled, the IP address restrictions are enforced for each page request, including requests from client applications.
5. If profile-based IP address restrictions are not set, Salesforce checks whether the user is logging in from a device used to access Salesforce before.
    - If the user's login is from a device and browser that Salesforce recognizes, the login is allowed.
    - If the user's login is from an IP address in your org's trusted IP address list, the login is allowed.
    - If the user's login is not from a trusted IP address or a device and browser Salesforce recognizes, the login is blocked.

Whenever a login is blocked or returns an API login fault, Salesforce has to verify the user's identity:

- For access via the user interface, the user is prompted to verify using Salesforce Authenticator (version 2 or later), or to enter a verification code.

  Note: Users aren't asked for a verification code the first time they log in to Salesforce.

- For access via the API or a client, users must add their security token to the end of their password to log in. Or, if "Two-Factor Authentication on API Logins" is set on the user profile, users enter a verification code generated by an authenticator app.

  A security token is an automatically generated key from Salesforce. For example, if a user's password is *`mypassword`*, and the security token is *`XXXXXXXXXX`*, the user must enter *`mypasswordXXXXXXXXXX`* to log in. Or some client applications have a separate field for the security token.

  Users can obtain their security token by changing their password or resetting their security token via the Salesforce user interface. When a user changes a password or resets a security token, Salesforce sends a new security token to the email address on the user's Salesforce record. The security token is valid until the user resets the security token, changes a password, or has a password reset.

  Tip: Before you access Salesforce from a new IP address, we recommend that you get your security token from a trusted network using **Reset My Security Token**.

Tips on Setting Login Restrictions

Consider the following when setting login restrictions.

- When a user's password is changed, the security token is reset. Log in via the API or a client can be blocked until the user adds the automatically generated security token to the end of the password.
- Partner Portal and Customer Portal users aren't required to activate their browser to log in.
- For more information on API login faults, see the Core Data Types Used in API Calls topic in the *SOAP API Developer's Guide*.
- If single sign-on (SSO) is enabled for your org, API and desktop client users can log in to Salesforce unless their profile has IP address restrictions set and they try to log in from outside of the range defined. Also the SSO authority usually handles login lockout policies for users with the "Is Single Sign-On Enabled" permission. However, if the security token is enabled for your org, your org's login lockout settings determine how many times users can attempt to log in with an invalid security token before being locked out of Salesforce.
- These events count toward the number of times users can attempt to log in with an invalid password before getting locked out of Salesforce, as defined in your org's login lockout settings.
  - Each time users are prompted to verify identity
  - Each time users incorrectly add the security token or verification code to the end of their password to log in to Salesforcevia the API or a client

IN THIS SECTION:

Restrict Login IP Ranges in the Enhanced Profile User Interface

Control login access at the user level by specifying a range of allowed IP addresses on a user's profile. When you define IP address restrictions for a profile, a login from any other IP address is denied.

Restrict Login IP Addresses in the Original Profile User Interface

Control login access at the user level by specifying a range of allowed IP addresses on a user's profile. When you define IP address restrictions for a profile, a login from any other IP address is denied.

View and Edit Login Hours in the Enhanced Profile User Interface

For each profile, you can specify the hours when users can log in.

View and Edit Login Hours in the Original Profile User Interface

Specify the hours when users can log in based on the user profile.

Set Trusted IP Ranges for Your Organization

Trusted IP Ranges define a list of IP addresses from which users can log in without receiving a login challenge for verification of their identity, such as a code sent to their mobile phone.

Two-Factor Authentication

As a Salesforce admin, you can enhance your org's security by requiring a second level of authentication for every user login. You can also require two-factor authentication when a user meets certain criteria, such as attempting to view reports or access a connected app.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

Salesforce Identity Verification

When a user logs in from outside a trusted IP range and uses a browser or app we don't recognize, the user is challenged to verify identity. We use the highest-priority verification method available for each user. In order of priority, the methods are:

1. Verification via push notification or location-based automated verification with the Salesforce Authenticator mobile app (version 2 or later) connected to the user's account.
2. Verification via a U2F security key registered with the user's account.
3. Verification code generated by a mobile authenticator app connected to the user's account.
4. Verification code sent via SMS to the user's verified mobile phone.
5. Verification code sent via email to the user's email address.

After identity verification is successful, the user doesn't have to verify identity again from that browser or app, unless the user:

- Manually clears browser cookies, sets the browser to delete cookies, or browses in private or incognito mode
- Deselects **Don't ask again** on the identity verification page

Org Policies That Require Two-Factor Authentication

You can set policies that require a second level of authentication on every login, every login through the API (for developers and client applications), or for access to specific features. Your users can provide the second factor by downloading and installing a mobile authenticator app, such as the Salesforce Authenticator app or the Google Authenticator app, on their mobile device. They can also use a U2F security key as the second factor. After they connect an authenticator app or register a security key with their account in Salesforce, they use them whenever your org's policies require two-factor authentication.

The Salesforce Authenticator mobile app (version 2 and later) sends a push notification to the user's mobile device when activity on the Salesforce account requires identity verification. The user responds on the mobile device to verify or block the activity. The user can enable location services for the app and automate verifications from trusted locations, such as a home or office. Salesforce Authenticator also generates verification codes, sometimes called "time-based one-time passwords" (TOTPs). Users can choose to enter a password plus the code instead of responding to a push notification from the app for two-factor verification. Or they can get a verification code from another authenticator app.

If users lose or forget the device they usually use for two-factor authentication, you can generate a temporary verification code for them. You set when the code expires, from 1 to 24 hours after you generate it. Your user can use the code multiple times until it expires. A user can have only one temporary code at a time. If a user needs a new code while the old code is still valid, you can expire the old code, then generate a new one. Users can expire their own valid codes in their personal settings.

SEE ALSO:

- Set Two-Factor Authentication Login Requirements
- Methods for Verifying Your Identity
- Restrict Where and When Users Can Log In to Salesforce
- Custom Login Flows
- Connect Salesforce Authenticator (Version 2 or Later) to Your Account for Identity Verification
- Verify Your Identity with a One-Time Password Generator App or Device
- Disconnect Salesforce Authenticator (Version 2 or Later) from a User's Account
- Disconnect a User's One-Time Password Generator App
- Generate a Temporary Identity Verification Code
- Expire a Temporary Verification Code
- Delegate Two-Factor Authentication Management Tasks
- Identity Verification History

Custom Login Flows

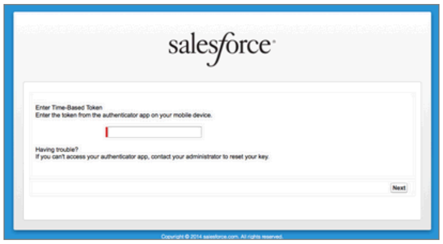
You can use a login flow to introduce business processes during login, such as to prompt for a second factor of authentication, accept terms of services, or collect information from users. After users complete the login flow, they're logged in to Salesforce.

Use the Cloud Flow Designer to create a flow. Then designate the flow as a login flow and associate it with specific profiles in your org. Users with the profile are directed to the login flow after they authenticate but before they can access your org. The login flow screens are embedded within the standard Salesforce login page for an integrated user login experience.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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



Enter Time-Based Token
Enter the token from the authenticator app on your mobile device.

Having trouble?
If you can't access your authenticator app, contact your administrator to reset your key.

Copyright © 2014 salesforce.com. All rights reserved.

Login flows support all the Salesforce UI authentication methods, including username and password, delegated authentication, SAML single sign-on, and social sign-on through a third-party authentication provider. You can apply login flows to Salesforce orgs and communities.

Note: You can't apply login flows to API logins or when sessions are passed to the UI through `frontdoor.jsp` from a non-UI login process. Only flows of type Flow are supported.

IN THIS SECTION:

[Create a Login Flow](#)

Use the Cloud Flow Designer to build a login flow. You use a login flow to direct users to perform a business process before they access Salesforce.

[Connect a Login Flow to Profiles](#)

After you create and activate a flow in Cloud Flow Designer, you designate it as a login flow and then associate it with profiles in your org. When users with an associated profile log in, they're directed to this login flow.

SEE ALSO:

[Cloud Flow Designer](#)

Create a Login Flow

Use the Cloud Flow Designer to build a login flow. You use a login flow to direct users to perform a business process before they access Salesforce.

For example, you can insert a form to gather more information from users when they log in. You can direct them to pages for other information, like terms of services. A common use for a login flow is to implement a custom two-factor authentication (2FA) process for increased security.

You create login flow screens with the Cloud Flow Designer. Then you embed the screens in the standard Salesforce login page from Setup. During the authentication process, the user is directed to the login flow screens. When users successfully authenticate and complete the login flow, they're redirected to Salesforce. The login process can also log out users immediately if necessary.

When you create a login flow for 2FA, you use Apex methods to get the session context, extract the user's IP address, and verify that the request is coming from a trusted IP range. If the request is coming from within a trusted IP range address, Salesforce skips the flow and logs the user in to the org. If the request is outside the IP range, Salesforce invokes the flow to:

- Direct the user to log in with additional credentials, such as a time-based one-time password (TOTP)
- Force the user to log out
- Direct the user to a page with more options

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To open, edit, or create a flow in the Cloud Flow Designer:

- Manage Force.com Flow

Build Your Own Login Flow

Use the following process to build your own login flow.

1. Create a flow using the Cloud Flow Designer and Apex.

   For example, you can design a custom IP-based 2FA flow that requires a second factor of authentication only if the user is logging in from outside of the trusted IP range.

   Note: To find or set the trusted IP range, from Setup, enter `Network Access` in the Quick Find box, then select **Network Access**.

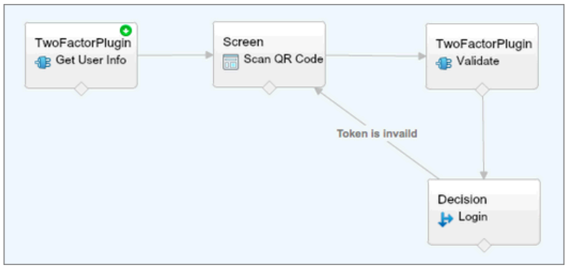
   Note: Don't set login IP ranges directly in a user profile. If you set the IP ranges in a profile, it restricts access for all users of that profile when they're outside the range. Then none of these users can enter the login flow process.

   Include the following in a flow.

   a. A new Apex class for defining an Apex plug-in. The plug-in implements from `Process.Plugin` and uses the `Auth.SessionManagement` class to access the time-based one-time password (TOTP) methods and services. The Apex class for the plug-in generates a time-based key with a quick response (QR) code to validate the TOTP provided by the user against the TOTP generated by Salesforce.

b. A screen element to scan a QR code.

c. A decision element to handle when the token is valid and invalid.



Use these input variables to populate the flow at startup.

Name	Value Description
`LoginFlow_LoginType`	Type of login, such as Application, OAuth, or SAML
`LoginFlow_IpAddress`	User's current IP address
`LoginFlow_LoginIpAddress`	User's IP address used during login, which can change after authentication
`LoginFlow_UserAgent`	User agent string provided by the user's browser
`LoginFlow_Platform`	User's operating system
`LoginFlow_Application`	Application used to request authentication
`LoginFlow_Community`	Current community if this login flow applies to a community
`LoginFlow_SessionLevel`	Current session security level, which can be STANDARD or HIGH_ASSURANCE
`LoginFlow_UserId`	User's 18-character ID

Use these variables to specify where the user goes after completing the flow.

Note: You must add a UI screen to the login flow to load these values. The login flow loads these values only after a UI screen is refreshed. A user clicking a button doesn't load the values.

Name	Description
`LoginFlow_FinishLocation`	String. Specify where in the org the user goes after completing the login flow. The string must be a relative path or a valid Salesforce URL. The login process can't redirect the user outside the org.

Name	Description
`LoginFlow_ForceLogout`	Boolean. Set this variable to `true` to log the user out immediately and force the user to exit the login flow.

2. Save the flow.
3. Activate the flow.
4. From the Login Flows Setup page, designate the flow as a login flow and connect it to profiles.

SEE ALSO:

Custom Login Flows

https://developer.salesforce.com/page/Login-Flows

Connect a Login Flow to Profiles

Cloud Flow Designer

Connect a Login Flow to Profiles

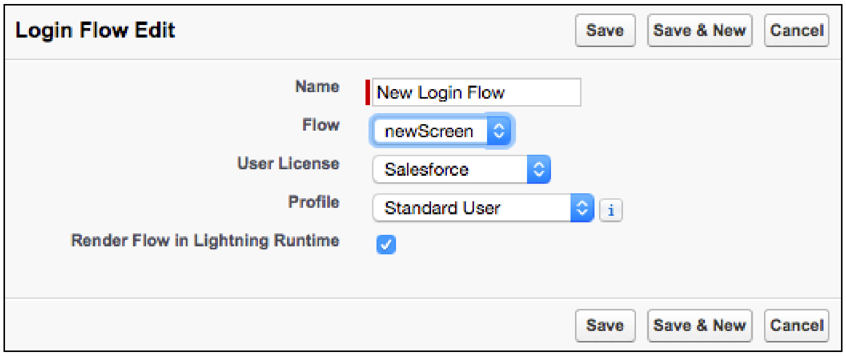
After you create and activate a flow in Cloud Flow Designer, you designate it as a login flow and then associate it with profiles in your org. When users with an associated profile log in, they're directed to this login flow.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

1. From Setup, enter `Login Flows` in the Quick Find box, then select **Login Flows**.
2. Click **New**.
3. On the Login Flow Edit page, enter a name for the login flow.



Login Flow Edit

Name: New Login Flow

Flow: newScreen

User License: Salesforce

Profile: Standard User

Render Flow in Lightning Runtime: ☑

4. Select the login flow from the dropdown list. The list contains flows created with the Cloud Flow Designer. Only active flows of type Flow are supported.
5. Select a user license for the profile that you want to connect to the login flow. When selected, a dropdown list contains the profiles available for the selected license.
6. From the dropdown list, select the profile to associate with the login flow.
7. If you want the login flow to resemble the Lightning Experience UI, select **Render Flow in Lightning Runtime**. If you don't select the option, the login flow resembles Salesforce Classic.

Note: A login flow is independent of which UI users use: Lightning Experience or Salesforce Classic. You can set a login flow to resemble Lightning Experience even if users log in to Salesforce Classic. Likewise, you can set a login flow to resemble Salesforce Classic even if users log in to Lightning Experience.

8. Click **Save**.

Repeat the process to associate other profiles with the login flow.

After you connect the login flow, you can edit or delete it from the Login Flows Setup page.

SEE ALSO:

Custom Login Flows

Create a Login Flow

Cloud Flow Designer

Configure User Authentication

Choose login settings to ensure that your users are who they say they are.

IN THIS SECTION:

Restrict Where and When Users Can Log In to Salesforce

You can restrict the hours during which users can log in and the range of IP addresses from which they can log in and access Salesforce. If IP address restrictions are defined for a user's profile and a login originates from an unknown IP address, Salesforce does not allow the login. These restrictions help protect your data from unauthorized access and phishing attacks.

Set Password Policies

Improve your Salesforce org security with password protection. You can set password history, length, and complexity requirements along with other values. In addition, you can specify what to do if a user forgets their password.

Expire Passwords for All Users

As an administrator, you can expire passwords for all users any time you want to enforce extra security for your organization. After expiring passwords, all users are prompted to reset their password the next time they log in.

Modify Session Security Settings

You can modify session security settings to specify session connection type, timeout settings, and IP address ranges to protect against malicious attacks and more.

Enable Lightning Login for Password-Free Logins

Say goodbye to the hassle of weak passwords, forgotten passwords, and locked-out accounts. Give your users the enhanced speed, convenience, and security of password-free logins. Enable Lightning Login, assign the required permission to your users, and encourage them to individually enroll in Lightning Login.

Create Logout Event Triggers (Pilot)

If the LogoutEventStream object is available to your org, you can create Apex triggers that respond to security logout events from your org's UI.

Create a Login Flow

Use the Cloud Flow Designer to build a login flow. You use a login flow to direct users to perform a business process before they access Salesforce.

Connect a Login Flow to Profiles

After you create and activate a flow in Cloud Flow Designer, you designate it as a login flow and then associate it with profiles in your org. When users with an associated profile log in, they're directed to this login flow.

Set Up Two-Factor Authentication

Admins enable two-factor authentication through permissions or profile settings. Users register devices for two-factor authentication—such as mobile authenticator apps or U2F security keys—through their own personal settings.

Restrict Where and When Users Can Log In to Salesforce

You can restrict the hours during which users can log in and the range of IP addresses from which they can log in and access Salesforce. If IP address restrictions are defined for a user's profile and a login originates from an unknown IP address, Salesforce does not allow the login. These restrictions help protect your data from unauthorized access and phishing attacks.

Login Hours

For each profile, you can set the hours when users can log in. See:

- View and Edit Login Hours in the Enhanced Profile User Interface
- View and Edit Login Hours in the Original Profile User Interface

Two-Factor Authentication for User Interface Logins

For each profile, you can require users to use a second form of authentication when they log in via the user interface. See Set Two-Factor Authentication Login Requirements on page 600 and Set Two-Factor Authentication Login Requirements and Custom Policies for Single Sign-On, Social Sign-On, and Communities.

Two-Factor Authentication for API Logins

For each profile, you can require a verification code (also called a time-based one-time password, or TOTP) instead of the standard security token. Users connect an authenticator app that generates verification codes to their account. Users with the "Two-Factor Authentication for API Logins" permission use a code instead of the standard security token whenever it's requested, such as when resetting the account's password. See Set Two-Factor Authentication Login Requirements for API Access on page 603.

Login IP Address Ranges

For Enterprise, Performance, Unlimited, Developer, and Database.com editions, you can set the Login IP Range addresses from which users can log in on an individual profile. Users outside of the Login IP Range set on a profile can't access your Salesforce org.

For Contact Manager, Group, and Professional Editions, set the Login IP Range. From Setup, enter *Session Settings* in the Quick Find box, then select **Session Settings**.

Login IP Address Range Enforcement for All Access Requests

You can restrict all access to Salesforce to the IP addresses included in Login IP Ranges in users' profiles. For example, suppose a user logs in successfully from an IP address defined in Login IP Ranges. The user then moves to a different location and has a new IP address that is outside of Login IP Ranges. When the user refreshes the browser or tries to access Salesforce, including access from a client application, the user is denied. To enable this option, from Setup, enter *Session Settings* in the Quick Find box, select **Session Settings**, and then select **Enforce login IP ranges on every request**. This option affects all user profiles that have login IP restrictions.

Org-wide Trusted IP Ranges

For all users, you can set a list of IP address ranges from which they can always log in without receiving a login challenge. These users can log in to your org after they provide the additional verification. See Set Trusted IP Ranges for Your Organization.

When users log in to Salesforce via the user interface, the API, or a desktop client such as Salesforce for Outlook, Connect Offline, Connect for Office, or the Data Loader, Salesforce confirms that the login is authorized as follows.

1. Salesforce checks whether the user's profile has login hour restrictions. If login hour restrictions are specified for the user's profile, any login outside the specified hours is denied.
2. If the user has the "Two-Factor Authentication for User Interface Logins" permission, Salesforce prompts the user for a second form of authentication upon logging in. If the user's account isn't already connected to a mobile authenticator app such as Salesforce Authenticator, Salesforce first prompts the user to connect the app.
3. If the user has the "Two-Factor Authentication for API Logins" permission and has connected an authenticator app to the account, Salesforce returns an error if the user uses the standard security token. The user has to enter a verification code (time-based one-time password) generated by the authenticator app instead.
4. Salesforce then checks whether the user's profile has IP address restrictions. If IP address restrictions are defined for the user's profile, logins from an undesignated IP address are denied, and logins from a specified IP address are allowed. If the **Enforce login IP ranges on every request** session setting is enabled, the IP address restrictions are enforced for each page request, including requests from client applications.
5. If profile-based IP address restrictions are not set, Salesforce checks whether the user is logging in from a device used to access Salesforce before.
   - If the user's login is from a device and browser that Salesforce recognizes, the login is allowed.
   - If the user's login is from an IP address in your org's trusted IP address list, the login is allowed.
   - If the user's login is not from a trusted IP address or a device and browser Salesforce recognizes, the login is blocked.

Whenever a login is blocked or returns an API login fault, Salesforce has to verify the user's identity:

- For access via the user interface, the user is prompted to verify using Salesforce Authenticator (version 2 or later), or to enter a verification code.

  Note: Users aren't asked for a verification code the first time they log in to Salesforce.

- For access via the API or a client, users must add their security token to the end of their password to log in. Or, if "Two-Factor Authentication on API Logins" is set on the user profile, users enter a verification code generated by an authenticator app.

  A security token is an automatically generated key from Salesforce. For example, if a user's password is `mypassword`, and the security token is `XXXXXXXXXX`, the user must enter `mypasswordXXXXXXXXXX` to log in. Or some client applications have a separate field for the security token.

  Users can obtain their security token by changing their password or resetting their security token via the Salesforce user interface. When a user changes a password or resets a security token, Salesforce sends a new security token to the email address on the user's Salesforce record. The security token is valid until the user resets the security token, changes a password, or has a password reset.

  Tip: Before you access Salesforce from a new IP address, we recommend that you get your security token from a trusted network using **Reset My Security Token**.

Tips on Setting Login Restrictions

Consider the following when setting login restrictions.

- When a user's password is changed, the security token is reset. Log in via the API or a client can be blocked until the user adds the automatically generated security token to the end of the password.

- Partner Portal and Customer Portal users aren't required to activate their browser to log in.
- For more information on API login faults, see the Core Data Types Used in API Calls topic in the *SOAP API Developer's Guide*.
- If single sign-on (SSO) is enabled for your org, API and desktop client users can log in to Salesforce unless their profile has IP address restrictions set and they try to log in from outside of the range defined. Also the SSO authority usually handles login lockout policies for users with the "Is Single Sign-On Enabled" permission. However, if the security token is enabled for your org, your org's login lockout settings determine how many times users can attempt to log in with an invalid security token before being locked out of Salesforce.
- These events count toward the number of times users can attempt to log in with an invalid password before getting locked out of Salesforce, as defined in your org's login lockout settings.
  - Each time users are prompted to verify identity
  - Each time users incorrectly add the security token or verification code to the end of their password to log in to Salesforcevia the API or a client

IN THIS SECTION:

Restrict Login IP Ranges in the Enhanced Profile User Interface

Control login access at the user level by specifying a range of allowed IP addresses on a user's profile. When you define IP address restrictions for a profile, a login from any other IP address is denied.

Restrict Login IP Addresses in the Original Profile User Interface

Control login access at the user level by specifying a range of allowed IP addresses on a user's profile. When you define IP address restrictions for a profile, a login from any other IP address is denied.

View and Edit Login Hours in the Enhanced Profile User Interface

For each profile, you can specify the hours when users can log in.

View and Edit Login Hours in the Original Profile User Interface

Specify the hours when users can log in based on the user profile.

Set Trusted IP Ranges for Your Organization

Trusted IP Ranges define a list of IP addresses from which users can log in without receiving a login challenge for verification of their identity, such as a code sent to their mobile phone.

Restrict Login IP Ranges in the Enhanced Profile User Interface

Control login access at the user level by specifying a range of allowed IP addresses on a user's profile. When you define IP address restrictions for a profile, a login from any other IP address is denied.

1. From Setup, enter *Profiles* in the `Quick Find` box, then select **Profiles**.
2. Select a profile and click its name.
3. In the profile overview page, click **Login IP Ranges**.
4. Specify allowed IP addresses for the profile.
   - To add a range of IP addresses from which users can log in, click **Add IP Ranges**. Enter a valid IP address in the `IP Start Address` and a higher-numbered IP address in the `IP End Address` field. To allow logins from only a single IP address, enter the same address in both fields.
   - To edit or remove ranges, click **Edit** or **Delete** for that range.

   Important:

   - The IP addresses in a range must be either IPv4 or IPv6. In ranges, IPv4 addresses exist in the IPv4-mapped IPv6 address space `::ffff:0:0` to `::ffff:ffff:ffff`, where `::ffff:0:0` is `0.0.0.0` and `::ffff:ffff:ffff` is `255.255.255.255`. A range can't include IP addresses both inside and outside of the IPv4-mapped IPv6 address space. Ranges like `255.255.255.255` to `::1:0:0:0` or `::` to `::1:0:0:0` aren't allowed.
   - Partner User profiles are limited to five IP addresses. To increase this limit, contact Salesforce.
   - The Salesforce Mobile Classic app can bypass IP ranges that are defined for profiles. Salesforce Mobile Classic initiates a secure connection to Salesforce over the mobile carrier's network. However, the mobile carrier's IP addresses can be outside of the IP ranges allowed for the user's profile. To prevent bypassing IP definitions on a profile, disable Salesforce Mobile Classic on page 870 for that user.

5. Optionally enter a description for the range. If you maintain multiple ranges, use the Description field to provide details, like which part of your network corresponds to this range.

Note: You can further restrict access to Salesforce to only those IPs in Login IP Ranges. To enable this option, in Setup, enter *Session Settings* in the `Quick Find` box, then select **Session Settings** and select **Enforce login IP ranges on every request**. This option affects all user profiles that have login IP restrictions.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view login IP ranges:
- View Setup and Configuration

To edit and delete login IP ranges:
- Manage Profiles and Permission Sets

Restrict Login IP Addresses in the Original Profile User Interface

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To view login IP ranges:

- View Setup and Configuration

To edit and delete login IP ranges:

- Manage Profiles and Permission Sets

Control login access at the user level by specifying a range of allowed IP addresses on a user's profile. When you define IP address restrictions for a profile, a login from any other IP address is denied.

1. How you restrict the range of valid IP addresses on a profile depends on your Salesforce edition.
   - If you're using an Enterprise, Unlimited, Performance, or Developer edition, from Setup, enter *`Profiles`* in the `Quick Find` box, then select **Profiles**, and select a profile.
   - If you're using a Professional, Group, or Personal edition, from Setup, enter *`Session Settings`* in the `Quick Find` box, then select **Session Settings**.
2. Click **New** in the Login IP Ranges related list.
3. Enter a valid IP address in the `IP Start Address` field and a higher-numbered IP address in the `IP End Address` field.

   The start and end addresses define the range of allowable IP addresses from which users can log in. To allow logins from a single IP address, enter the same address in both fields.
   - The IP addresses in a range must be either IPv4 or IPv6. In ranges, IPv4 addresses exist in the IPv4-mapped IPv6 address space `::ffff:0:0` to `::ffff:ffff:ffff`, where `::ffff:0:0` is `0.0.0.0` and `::ffff:ffff:ffff` is `255.255.255.255`. A range can't include IP addresses both inside and outside of the IPv4-mapped IPv6 address space. Ranges like `255.255.255.255` to `::1:0:0:0` or `::` to `::1:0:0:0` aren't allowed.
   - Partner User profiles are limited to five IP addresses. To increase this limit, contact Salesforce.
   - The Salesforce Mobile Classic app can bypass IP ranges that are defined for profiles. Salesforce Mobile Classic initiates a secure connection to Salesforce over the mobile carrier's network. However, the mobile carrier's IP addresses can be outside of the IP ranges allowed for the user's profile. To prevent bypassing IP definitions on a profile, disable Salesforce Mobile Classic on page 870 for that user.
4. Optionally enter a description for the range. If you maintain multiple ranges, use the Description field to provide details, such as which part of your network corresponds to this range.
5. Click **Save**.

Note: Cache settings on static resources are set to private when accessed via a Force.com site whose guest user's profile has restrictions based on IP range or login hours. Sites with guest user profile restrictions cache static resources only within the browser. Also, if a previously unrestricted site becomes restricted, it can take up to 45 days for the static resources to expire from the Salesforce cache and any intermediate caches.

Note: You can further restrict access to Salesforce to only those IPs in Login IP Ranges. To enable this option, in Setup, enter *`Session Settings`* in the `Quick Find` box, then select **Session Settings** and select **Enforce login IP ranges on every request**. This option affects all user profiles that have login IP restrictions.

SEE ALSO:

Set Trusted IP Ranges for Your Organization

View and Edit Login Hours in the Original Profile User Interface

Work in the Original Profile Interface

View and Edit Login Hours in the Enhanced Profile User Interface

For each profile, you can specify the hours when users can log in.

1. From Setup, enter `Profiles` in the `Quick Find` box, then select **Profiles**.
2. Select a profile and click its name.
3. In the profile overview page, scroll down to Login Hours and click **Edit**.
4. Set the days and hours when users with this profile can log in to the organization.

   To allow users to log in at any time, click **Clear all times**. To prohibit users from using the system on a specific day, set the start and end times to the same value.

   If users are logged in when their login hours end, they can continue to view their current page, but they can't take any further action.

> Note: The first time login hours are set for a profile, the hours are based on the organization's `Default Time Zone` as specified on the Company Information page in Setup. After that, any changes to the organization's `Default Time Zone` won't change the time zone for the profile's login hours. As a result, the login hours are always applied at those exact times even if a user is in a different time zone or if the organization's default time zone is changed.
>
> Depending on whether you're viewing or editing login hours, the hours may appear differently. On the Login Hours edit page, hours are shown in your specified time zone. On the profile overview page, they appear in the organization's original default time zone.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view login hour settings:
- View Setup and Configuration

To edit login hour settings:
- Manage Profiles and Permission Sets

SEE ALSO:

Enhanced Profile User Interface Overview

View and Edit Login Hours in the Original Profile User Interface

Specify the hours when users can log in based on the user profile.

1. From Setup, enter `Profiles` in the `Quick Find` box, then select **Profiles**, and select a profile.
2. Click **Edit** in the Login Hours related list.
3. Set the days and hours when users with this profile can use the system.

   To allow users to log in at any time, click **Clear All Times**. To prohibit users from using the system on a specific day, set the start and end times to the same value.

   If users are logged in when their login hours end, they can continue to view their current page, but they can't take any further action.
4. Click **Save**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To set login hours:
- Manage Profiles and Permission Sets

Note: The first time login hours are set for a profile, the hours are based on the organization's `Default Time Zone` as specified on the Company Information page in Setup. After that, any changes to the organization's `Default Time Zone` won't change the time zone for the profile's login hours. As a result, the login hours are always applied at those exact times even if a user is in a different time zone or if the organization's default time zone is changed.

Depending on whether you're viewing or editing login hours, the hours appear differently. On the profile detail page, hours are shown in your specified time zone. On the Login Hours edit page, they appear in the organization's default time zone.

SEE ALSO:

Work in the Original Profile Interface

Restrict Login IP Addresses in the Original Profile User Interface

Set Trusted IP Ranges for Your Organization

Trusted IP Ranges define a list of IP addresses from which users can log in without receiving a login challenge for verification of their identity, such as a code sent to their mobile phone.

Note: ▶ Who Sees What: Organization Access (English only)

Watch how you can restrict login through IP ranges and login hours.

To help protect your organization's data from unauthorized access, you can specify a list of IP addresses from which users can log in without receiving a login challenge. However, this does not restrict access, entirely, for users outside of the Trusted IP Range. After these users complete the login challenge (usually by entering a code sent to their mobile device or email address), they can log in.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To change network access:

- Manage IP Addresses

1. From Setup, enter *`Network Access`* in the `Quick Find` box, then select **Network Access**.
2. Click **New**.
3. Enter a valid IP address in the `Start IP Address` field and a higher IP address in the `End IP Address` field.

   The start and end addresses define the range of allowable IP addresses from which users can log in, including the start and end values. If you want to allow logins from a single IP address, enter the same address in both fields.

   The start and end IP addresses must be in an IPv4 range and include no more than 33,554,432 addresses (2^{25}, a /7 CIDR block).
4. Optionally, enter a description for the range. For example, if you maintain multiple ranges, enter details about the part of your network that corresponds to this range.
5. Click **Save**.

Note: For organizations that were activated before December 2007, Salesforce automatically populated your organization's trusted IP address list in December 2007, when this feature was introduced. The IP addresses from which trusted users had already accessed Salesforce during the past six months were added.

SEE ALSO:

Session Security

Restrict Where and When Users Can Log In to Salesforce

Security Implementation Guide

Set Password Policies

Improve your Salesforce org security with password protection. You can set password history, length, and complexity requirements along with other values. In addition, you can specify what to do if a user forgets their password.

For your organization's security, you can set various password and login policies.

> Note: User passwords cannot exceed 16,000 bytes.
>
> Logins are limited to 3,600 per hour per user. This limit applies to organizations created after Summer '08.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To set password policies:
- Manage Password Policies

1. From Setup, enter *`Password Policies`* in the `Quick Find` box, then select **Password Policies**.
2. Customize the password settings.

Field	Description
`User passwords expire in`	The length of time until user passwords expire and must be changed. The default is 90 days. This setting isn't available for Self-Service portals. This setting doesn't apply to users with the "Password Never Expires" permission. If you change the `User passwords expire in` setting, the change affects a user's password expiration date if that user's new expiration date is earlier than the old expiration date or if you remove an expiration by selecting `Never expires`.
`Enforce password history`	Save users' previous passwords so that they must always reset their password to a new, unique password. Password history is not saved until you set this value. The default is `3 passwords remembered`. You cannot select `No passwords remembered` unless you select `Never expires` for the `User passwords expire in` field. This setting isn't available for Self-Service portals.
`Minimum password length`	The minimum number of characters required for a password. When you set this value, existing users aren't affected until the next time they change their passwords. The default is `8 characters`.

Field	Description
`Password complexity requirement`	The requirement for which types of characters must be used in a user's password. Complexity levels: • `No restriction`—allows any password value and is the least secure option. • `Must mix alpha and numeric characters`—requires at least one alphabetic character and one number, which is the default. • `Must mix alpha, numeric, and special characters`—requires at least one alphabetic character, one number, and one of the following special characters: *! # $ % - _ = + < >*. • `Must mix numbers and uppercase and lowercase letters`—requires at least one number, one uppercase letter, and one lowercase letter. • `Must mix numbers, uppercase and lowercase letters, and special characters`—requires at least one number, one uppercase letter, and one lowercase letter, and one of the following special characters: *! # $ % - _ = + < >*. Note: Only the special characters listed meet the requirement. Other symbol characters are not considered special characters.
`Password question requirement`	The values are `Cannot contain password`, meaning that the answer to the password hint question cannot contain the password itself; or `None`, the default, for no restrictions on the answer. The user's answer to the password hint question is required. This setting is not available for Self-Service portals, Customer Portals, or partner portals.
`Maximum invalid login attempts`	The number of login failures allowed for a user before they become locked out. This setting isn't available for Self-Service portals.
`Lockout effective period`	The duration of the login lockout. The default is 15 minutes. This setting isn't available for Self-Service portals. Note: If users are locked out, they must wait until the lockout period expires. Alternatively, a user with the "Reset User Passwords and Unlock Users" permission can unlock them from Setup with the following procedure: **a.** Enter *`Users`* in the `Quick Find` box. **b.** Select **Users**. **c.** Selecting the user.

Field	Description
	d. Click **Unlock**. This button is only available when a user is locked out.
`Obscure secret answer for password resets`	This feature hides answers to security questions as you type. The default is to show the answer in plain text. Note: If your org uses the Microsoft Input Method Editor (IME) with the input mode set to Hiragana, when you type ASCII characters, they're converted in Japanese characters in normal text fields. However, the IME doesn't work properly in fields with obscured text. If your org's users cannot properly enter their passwords or other values after enabling this feature, disable the feature.
`Require a minimum 1 day password lifetime`	When you select this option, a password can't be changed more than once in a 24-hour period.

3. Customize the forgotten password and locked account assistance information.

   Note: This setting is not available for Self-Service portals, Customer Portals, or partner portals.

Field	Description
`Message`	If set, this message appears in the "We can't reset your password" email. Users receive this email when they lock themselves out by trying to reset their password too many times. The text also appears at the bottom of the Answer Your Security Question page when users reset their passwords. You can tailor the text to your organization by adding the name of your internal help desk or a system administrator. For the email, the message appears only for accounts that need an administrator to reset them. Lockouts due to time restrictions get a different system email message.
`Help link`	If set, this link displays with the text defined in the `Message` field. In the "We can't reset your password" email, the URL displays exactly as typed in the `Help link` field, so the user can see where the link goes. This URL display format is a security feature, because the user is not within a Salesforce organization. On the Answer Your Security Question page, the `Help link` URL combines with the text in the `Message` field to make a clickable link. Security isn't an issue, because the user is in a Salesforce organization when changing passwords. Valid protocols:

Field	Description
	• http • https • mailto

4. Specify an alternative home page for users with the "API Only User" permission. After completing user management tasks such as resetting a password, API-only users are redirected to the URL specified here, rather than to the login page.
5. Click **Save**.

SEE ALSO:

View and Edit Password Policies in Profiles

Passwords

Expire Passwords for All Users

As an administrator, you can expire passwords for all users any time you want to enforce extra security for your organization. After expiring passwords, all users are prompted to reset their password the next time they log in.

To expire passwords for all users, except those users with the "Password Never Expires" permission:

1. From Setup, enter `Expire All Passwords` in the `Quick Find` box, then select **Expire All Passwords**.
2. Select **Expire all user passwords**.
3. Click **Save**.

The next time users log in, they are prompted to reset their password.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To expire all passwords:
- Reset User Passwords and Unlock Users

Considerations When Expiring Passwords

- Users might need to activate their computers to log in to Salesforce.
- `Expire all user passwords` doesn't affect Self-Service portal users, because they aren't direct Salesforce users.

SEE ALSO:

Passwords

Modify Session Security Settings

You can modify session security settings to specify session connection type, timeout settings, and IP address ranges to protect against malicious attacks and more.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

The `Lock sessions to the IP address from which they originated` setting is available in: **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

All other settings available in: **Essentials**, **Personal**, **Contact Manager**, **Group**, **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

USER PERMISSIONS

To modify session security settings:

- Customize Application

1. From Setup, enter `Session Settings` in the Quick Find box, then select **Session Settings**.
2. Customize the session security settings.

Field	Description
`Timeout value`	Length of time after which the system logs out inactive users. For Portal users, the timeout is between 10 minutes and 24 hours even though you can only set it as low as 15 minutes. Select a value between 15 minutes and 24 hours. Choose a shorter timeout period if your org has sensitive information and you want to enforce stricter security. Note: The last active session time value isn't updated until halfway through the timeout period. So if you have a 30-minute timeout, the system doesn't check for activity until 15 minutes have passed. For example, if you update a record after 10 minutes, the last active session time value isn't updated because there was no activity after 15 minutes. You're logged out in 20 more minutes (30 minutes total), because the last active session time wasn't updated. Suppose that you update a record after 20 minutes. That's 5 minutes after the last active session time is checked. Your timeout resets, and you have another 30 minutes before being logged out, for a total of 50 minutes.
`Disable session timeout warning popup`	Determines whether the system prompts inactive users with a timeout warning message. Users are prompted 30 seconds before timeout as specified by the `Timeout value`.
`Force logout on session timeout`	Requires that when sessions time out for inactive users, current sessions become invalid. The browser refreshes and returns to the login page. To access the org, the user must log in again. Note: Do *not* select `Disable session timeout warning popup` when using this setting.
`Lock sessions to the IP address from which they originated`	Determines whether user sessions are locked to the IP address from which the user logged in, helping to prevent unauthorized persons from hijacking a valid session.

Field	Description
	Note: This setting can inhibit various applications and mobile devices.
Lock sessions to the domain in which they were first used	Associates a current UI session for a user, such as a community user, with a specific domain. The setting helps prevent unauthorized use of the session ID in another domain. This setting is enabled by default for orgs created with the Spring '15 release or later.
Require secure connections (HTTPS)	Determines whether HTTPS is required to log in to or access Salesforce. This setting is enabled by default for security reasons. This setting does not apply to API requests. All API requests require HTTPS. To enable HTTPS on communities and Force.com sites see: HSTS for Sites and Communities Note: The Reset Passwords for Your Users page can only be accessed using HTTPS.
Require secure connections (HTTPS) for all third-party domains	Determines whether HTTPS is required for connecting to third-party domains. This setting is enabled by default on accounts created after the Summer '17 release.
Force relogin after Login-As-User	Determines whether an administrator who is logged in as another user is returned to their previous session after logging out as the secondary user. If the setting is enabled, an administrator must log in again to continue using Salesforce after logging out as the user. Otherwise, the administrator is returned to the original session after logging out as the user. This setting is enabled by default for new orgs beginning with the Summer '14 release.
Require HttpOnly attribute	Restricts session ID cookie access. A cookie with the HttpOnly attribute is not accessible via non-HTTP methods, such as calls from JavaScript. Note: If you have a custom or packaged application that uses JavaScript to access session ID cookies, selecting Require HttpOnly attribute breaks your application. It denies the application access to the cookie. If Require HttpOnly attribute is selected, the AJAX Toolkit debugging window isn't available.

Use POST requests for cross-domain sessions	Sets the org to send session information using a POST request, instead of a GET request, for cross-domain exchanges. An example of a cross-domain exchange is when a user is using a Visualforce page. In this context, POST requests are more secure than GET requests because POST requests keep the session information in the body of the request. However, if you enable this setting, embedded content from another domain, such as:
	`<img`
	`src="https://acme.force.com/pic.jpg"/>`

Field	Description
	sometimes doesn't display.
`Enforce login IP ranges on every request`	Restricts the IP addresses from which users can access Salesforce to only the IP addresses defined in `Login IP Ranges`. If this setting is enabled, login IP ranges are enforced on each page request, including requests from client applications. If this setting isn't enabled, login IP ranges are enforced only when a user logs in. This setting affects all user profiles that have login IP restrictions.
`Enable caching and autocomplete on login page`	Allows the user's browser to store usernames. If enabled, after initial login, usernames are auto-filled into the `Username` field on the login page. If the user selected **Remember me** on the login page, the username persists after the session expires or the user logs out. The username also appears on the Switcher. This setting is selected by default for all orgs. Note: If you disable this setting, the **Remember me** option doesn't appear on your org's login page or from the Switcher.
`Enable secure and persistent browser caching to improve performance`	Enables secure data caching in the browser to improve page reload performance by avoiding extra round trips to the server. This setting is selected by default for all orgs. We don't recommend disabling this setting, but if your company's policy doesn't allow browser caching even if the data is encrypted, you can disable it.
`Enable user switching`	Determines whether the Switcher appears when your org's users select their profile picture. This setting is selected by default for all organizations. The `Enable caching and autocomplete on login page` setting must also be enabled. Deselect the `Enable user switching` setting to prevent your org from appearing in Switchers on other orgs. It also prevents your org users from seeing the Switcher when they select their profile picture.
`Remember until logout`	Normally, usernames are cached only while a session is active or if a user selects **Remember Me**. For SSO sessions, the remember option isn't available. So, once the session expires, the username disappears from the login page and the Switcher. By enabling `Remember me until logout`, the cached usernames are deleted only if the user explicitly logs out. If the session times out, they appear on the Switcher as inactive. This way, if the users are on their own computer and allow a session to timeout, they can select the username to reauthenticate. If they're on a shared computer, the username is deleted immediately when the user logs out. This setting applies to all your org's users. This option isn't enabled by default. However, we encourage you to enable it as a convenience to your users. Keep this setting disabled if your org doesn't expose all your SSO or authentication providers on your login page.
`Enable the SMS method of identity confirmation`	Allows users to receive a one-time PIN delivered via SMS. If this setting is selected, administrators or users must verify their mobile phone number before taking advantage of this feature. This setting is selected by default for all orgs.

Field	Description
`Require security tokens for API logins from callouts (API version 31.0 and earlier)`	In API version 31.0 and earlier, requires the use of security tokens for API logins from callouts. Examples are Apex callouts or callouts using the AJAX proxy. In API version 32.0 and later, security tokens are required by default.
`Login IP Ranges` (for Contact Manager, Group, and Professional Editions)	Specifies a range of IP addresses users must log in from (inclusive), or the login fails. To specify a range, click **New** and enter a Start IP Address and End IP Address to define the range, which includes the start and end values. This field is not available in Enterprise, Unlimited, Performance, and Developer Editions. In those editions, you can specify a valid Login IP Range in the user profile settings.
`Let users use a security key (U2F)`	Allows users to use a U2F security key for two-factor authentication and identity verification. Instead of using Salesforce Authenticator, a one-time password generated by an authenticator app, or one-time passwords sent by email or SMS, users insert their registered U2F security key into a USB port to complete verification.
`Require identity verification during two-factor authentication registration`	Requires users to confirm their identities to add a two-factor authentication method, such as Salesforce Authenticator, instead of requiring a relogin as before.
`Require identity verification for change of email address`	Requires users to confirm their identities to change email addresses instead of requiring a relogin as before. Note: To get the emails to confirm identity, make sure that users have access to their previously registered email accounts.

`Allow location-based automated verifications with Salesforce Authenticator`
`Allow only from trusted IP addresses`
	Allows users to verify identity by automatically approving notifications in Salesforce Authenticator, whenever users are in trusted locations such as a home or office. If you allow automated verifications, you can allow them from any location or restrict them to only trusted IP addresses, such as your corporate network.

`Allow Lightning Login`	Allows users to use Lightning Login for password-free Salesforce logins, relying on Salesforce Authenticator for identity verification.
`Enable clickjack protection for Setup pages`	Protects against clickjack attacks on setup Salesforce pages. Clickjacking is also known as a user interface redress attack. (Setup pages are available from the Setup menu.)
`Enable clickjack protection for non-Setup Salesforce pages`	Protects against clickjack attacks on non-setup Salesforce pages. Clickjacking is also known as a user interface redress attack. Setup pages already include protection against clickjack attacks. (Setup pages are available from the Setup menu.) This setting is selected by default for all orgs.

Field	Description
`Enable clickjack protection for customer Visualforce pages with standard headers`	Protects against clickjack attacks on your Visualforce pages with headers enabled. Clickjacking is also known as a user interface redress attack. Warning: If you use custom Visualforce pages within a frame or iframe, you sometimes see a blank page or the page displays without the frame. For example, Visualforce pages in a page layout don't function when clickjack protection is on.
`Enable clickjack protection for customer Visualforce pages with headers disabled`	Protects against clickjack attacks on your Visualforce pages with headers disabled when setting `showHeader="false"` on the page. Clickjacking is also known as a user interface redress attack. Warning: If you use custom Visualforce pages within a frame or iframe, you sometimes see a blank page or the page displays without the frame. For example, Visualforce pages in a page layout don't function when clickjack protection is on.
`Enable CSRF protection on GET requests on non-setup pages`	Protects against Cross Site Request Forgery (CSRF) attacks by modifying non-Setup pages. Non-Setup pages include a random string of characters in the URL parameters or as a hidden form field. With every GET and POST request, the application checks the validity of this string of characters. The application doesn't execute the command unless the value found matches the expected value. This setting is selected by default for all orgs.
`Enable CSRF protection on POST requests on non-setup pages`	
`XSS protection`	Protects against reflected cross-site scripting attacks. If a reflected cross-site scripting attack is detected, the browser shows a blank page with no content.
`Content Sniffing protection`	Prevents the browser from inferring the MIME type from the document content. It also prevents the browser from executing malicious files (JavaScript, Stylesheet) as dynamic content.
`Referrer URL Protection`	When loading pages, the referrer header shows only Salesforce.com rather than the entire URL. This feature eliminates the potential for a referrer header to reveal sensitive information that could be present in a full URL, such as an org ID. This feature is supported only for Chrome and Firefox.
`HSTS for Sites and Communities`	Requires HTTPS on communities and Force.com sites. Note: This setting must be enabled in two locations. `HSTS for Sites and Communities` must be enabled in Session Settings, and `Require Secure Connections (HTTPS)` must be enabled in the community or Force.com site security settings. See Creating and Editing Force.com Sites.
`Logout URL`	Redirects users to a specific page after they log out of Salesforce, such as an authentication provider's page or a custom-branded page. This URL is used only if no logout URL is specified in the identity provider, SAML single sign-on, or external authentication provider settings. If no value is specified for `Logout URL`, the default is `https://login.salesforce.com`, unless

Field	Description
	MyDomain is enabled. If My Domain is enabled, the default is `https://`*`customdomain`*`.my.salesforce.com`.

3. Click **Save**.

Session Security Levels

You can restrict access to certain types of resources based on the level of security associated with the authentication (login) method for the user's current session. By default, each login method has one of two security levels: Standard or High Assurance. You can change the session security level and define policies so specified resources are only available to users with a High Assurance level.

The different authentication methods are assigned these security levels, by default.

- Username and Password — Standard
- Delegated Authentication — Standard
- Activation — Standard
- Lightning Login — Standard
- Two-Factor Authentication — High Assurance
- Authentication Provider — Standard
- SAML — Standard

Note: The security level for a SAML session can also be specified using the `SessionLevel` attribute of the SAML assertion sent by the identity provider. The attribute can take one of two values, `STANDARD` or `HIGH_ASSURANCE`.

To change the security level associated with a login method:

1. From Setup, enter *`Session Settings`* in the `Quick Find` box, then select **Session Settings**.
2. Under Session Security Levels, select the login method.
3. To move the method to the proper category, click the **Add** or **Remove** arrow.

Currently, the only features that use session-level security are reports and dashboards in Salesforce and connected apps. You can set policies requiring High Assurance on these types of resources. You can also specify an action to take if the session used to access the resource is not High Assurance. The supported actions are:

- Block — Blocks access to the resource by showing an insufficient privileges error.
- Raise session level — Prompts users to complete two-factor authentication. When users authenticate successfully, they can access the resource. For reports and dashboards, you can apply this action when users access reports or dashboards, or just when they export and print them.

Warning: Raising the session level to high assurance by redirecting the user to complete two-factor authentication is not a supported action in Lightning Experience. If your org has Lightning Experience enabled, and you set a policy that requires a high assurance session to access reports and dashboards, Lightning Experience users with a standard assurance session are blocked from reports and dashboards. Also, they don't see the icons for these resources in the navigation menu. As a workaround, users with a standard assurance session can log out and log in again using an authentication method that is defined as high assurance by their org. Then they have access to reports and dashboards. Or, they can switch to Salesforce Classic, where they're prompted to raise the session level when they attempt to access reports and dashboards.

To set a High Assurance required policy for accessing a connected app:

1. From Setup, enter *`Connected Apps`* in the `Quick Find` box, then select the option for managing connected apps.

2. Click **Edit** next to the connected app.
3. Select **High Assurance session required**.
4. Select one of the actions presented.
5. Click **Save**.

To set a High Assurance required policy for accessing reports and dashboards:

1. From Setup, enter `Access Policies` in the `Quick Find` box, then select **Access Policies**.
2. Select **High Assurance session required**.
3. Select one of the actions presented.
4. Click **Save**.

Session levels have no impact on resources in the app other than connected apps, reports, and dashboards for which explicit security policies have been defined.

SEE ALSO:

Session Security

Explore the Salesforce Setup Menu

Identity Verification History

Enable Lightning Login for Password-Free Logins

Say goodbye to the hassle of weak passwords, forgotten passwords, and locked-out accounts. Give your users the enhanced speed, convenience, and security of password-free logins. Enable Lightning Login, assign the required permission to your users, and encourage them to individually enroll in Lightning Login.

Password-free logins rely on Salesforce Authenticator (version 2 or later), the two-factor authentication mobile app that's available as a free download for iOS and Android devices. Lightning Logins add a layer of security by requiring two factors of authentication for login.

- The first factor is something that the user has—a mobile device that has Salesforce Authenticator installed and connected with the user's Salesforce account.
- The second factor is something that the user is, such as a fingerprint, or something that the user knows, such as a PIN. The second level of authentication enhances security by requiring access to the mobile device and the user's fingerprint or PIN.

Lightning Login isn't limited to orgs using Lightning Experience. It works in Salesforce Classic, too.

All internal users (not external community users) are eligible for Lightning Login by default, but you can decide whether to make it available to all users. You can also determine user eligibility by using the Lightning Login User permission.

1. From Setup, enter `Session Settings` in the Quick Find box, then select **Session Settings**.
2. Review the default settings for Lightning Login.
   a. Make sure that **Allow Lightning Login** is enabled.

      You can disable Allow Lightning Login at any time to switch users back to username and password logins.

   b. Decide if you want to make Lightning Login available to all users or only users with the Lightning Login User permission.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

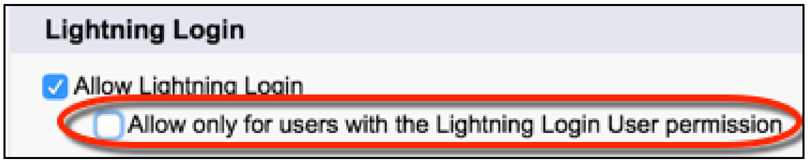
USER PERMISSIONS

To edit system permissions in profiles:

- Manage Profiles and Permission Sets

To enable Lightning Login:

- Customize Application



Lightning Login

☑ Allow Lightning Login

□ Allow only for users with the Lightning Login User permission

c. Confirm that a Standard session security level is appropriate for this login method.

   Lightning Login establishes a Standard security level for the user's session. Standard is the default security level for the Username Password method that Lightning Login typically replaces. If needed, you can change the security level to High Assurance.

3. Assign the Lightning Login User permission to users in the user profile (for cloned or custom profiles only) or permission set. Lightning Login isn't supported for external users.

Consider these points about how Lightning Login relates to other login, identity verification, and two-factor authentication features.

- You can monitor your users' Lightning Login activity using Login History or Identity Verification History tools.
- If enrolled users attempt a Lightning Login from an unrecognized browser or device, Salesforce requires login using username and password, along with identity verification.
- If an enrolled user previously logged in from a browser and selected **Remember me**, login hints on the login page show a lightning bolt next to past usernames that are Lightning Login–enabled.

  Note: For Lightning Login to display login hints properly in the Apple Safari browser, change the **Cookies and website data** option in the browser. Advise your users to change it from **Allow from websites I visit** to **Always allows**.

- If your org sets a two-factor authentication policy for logins, the Lightning Login method satisfies the second factor requirement. Salesforce does not separately require users with the Two-Factor Authentication for User Interface Logins permission to provide a second factor.
- If your org has defined a transaction security policy that requires two-factor authentication, Lightning Login isn't supported. Enrolled users who attempt a Lightning Login must use log in with username and password instead.

IN THIS SECTION:

Enroll in Lightning Login for Password-Free Logins

Enroll in Lightning Login so that you can enjoy the enhanced speed, convenience, and security of password-free logins.

Cancel a User's Lightning Login Enrollment

Cancel a user's Lightning Login enrollment if the user is no longer eligible to use Lightning Login.

Enroll in Lightning Login for Password-Free Logins

Enroll in Lightning Login so that you can enjoy the enhanced speed, convenience, and security of password-free logins.

If a Salesforce admin has made you eligible to enroll in Lightning Login, enroll yourself (an admin can't enroll for you).

1. Have your mobile device in hand so that you're ready to approve the enrollment notification.

   Lightning Login requires Salesforce Authenticator (version 2 or later), the two-factor authentication mobile app that's available as a free download for iOS and Android devices. If you aren't already using Salesforce Authenticator, enrollment includes a few extra steps. You're guided through downloading and installing Salesforce Authenticator, connecting it to your Salesforce account, and setting up a second factor of authentication (a fingerprint or PIN).

2. From your personal settings, enter *`Advanced User Details`* in the `Quick Find` box, then select **Advanced User Details**. No results? Enter *`Personal Information`* in the `Quick Find` box, then select **Personal Information**.
3. Click **Enroll** next to the `Lightning Login` field.

   If you don't see this option, your admin hasn't made you eligible to enroll.

4. At the prompt, check the Salesforce Authenticator notification on your mobile device and approve the request.
5. At the prompt, provide your fingerprint or PIN on the mobile device.

Now you're ready to use this login method.

1. **Click**—On the Salesforce login page, look for the lightning bolt next to your Lightning Login–enabled username, and click your username. If the login page asks for both username and password, you can enter only your username, skip the password field, and click **Log In**.
2. **Tap**—On your mobile device, tap the notification from the Salesforce Authenticator app.
3. **Touch**—Verify your identity with your fingerprint or PIN. Presto! You're logged in.

While enrolled, if you're ever without your mobile device, you can still log in with your username and password. If you disconnect Salesforce Authenticator from your Salesforce account, Lightning Login isn't allowed until you connect Salesforce Authenticator again.

You can cancel your enrollment at any time, and so can an admin.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To enroll in Lightning Login:
- Lightning Login User

Cancel a User's Lightning Login Enrollment

Cancel a user's Lightning Login enrollment if the user is no longer eligible to use Lightning Login.

1. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.
2. Click the user's name.
3. On the user's detail page, click **Cancel** next to the `Lightning Login` field.

Your users can cancel their own enrollment. In personal settings, they go to the Advanced User Details page and click **Cancel** next to the `Lightning Login` field.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To cancel a user's Lightning Login enrollment:

- Manage Users

Create Logout Event Triggers (Pilot)

If the LogoutEventStream object is available to your org, you can create Apex triggers that respond to security logout events from your org's UI.

EDITIONS

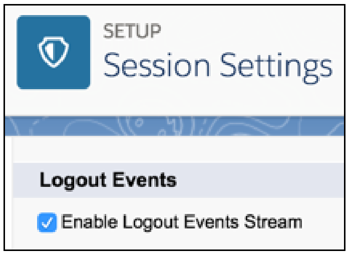
Available in all editions

Note: We provide enabling of logout event triggers to selected customers through a pilot program that requires agreement to specific terms and conditions. These terms and conditions apply to the use of the LogoutEventStream object. To be nominated to participate in the program, contact Salesforce. Pilot programs are subject to change, and we can't guarantee acceptance. LogoutEventStream isn't generally available unless or until Salesforce announces its general availability in documentation or in press releases or public statements. We can't guarantee general availability within any particular time frame or at all. Make your purchase decisions only on the basis of generally available products and features. You can provide feedback and suggestions for the LogoutStreamEvent object and for enabling logout event triggers in the Salesforce Identity group in the Trailblazer Community.

To enable the LogoutStreamEvent object, contact Salesforce Customer Support.

After LogoutEventStream is enabled, Salesforce publishes logout events when users log out from the UI. You can add an Apex trigger to subscribe to those events. You can then implement custom logic during logout. For example, you can revoke all refresh tokens for a user at logout.

1. If Salesforce Customer Service has enabled LogoutStreamEvent for your org, from Setup, enter `Session Settings` in the `Quick Find` box, then select **Session Settings**.
2. Under **Logout Events**, select **Enable Logout Events Stream**.


SETUP
Session Settings

Logout Events

☑ Enable Logout Events Stream

3. Create Apex triggers that subscribe to logout events.

Example: In this example, the subscriber inserts a custom logout event record during logout.

```
trigger LogoutEventTrigger on LogoutEventStream (after insert) {
  LogoutEventStream event = Trigger.new[0];
  LogoutEvent__c record = new LogoutEvent__c();
  record.EventIdentifier__c = event.EventIdentifier;
  record.UserId__c = event.UserId;
  record.Username__c = event.Username;
  record.EventDate__c = event.EventDate;
  record.RelatedEventIdentifier__c = event.RelatedEventIdentifier;
  record.SessionKey__c = event.SessionKey;
  record.LoginKey__c = event.LoginKey;
  insert(record);
}
```

Create a Login Flow

Use the Cloud Flow Designer to build a login flow. You use a login flow to direct users to perform a business process before they access Salesforce.

For example, you can insert a form to gather more information from users when they log in. You can direct them to pages for other information, like terms of services. A common use for a login flow is to implement a custom two-factor authentication (2FA) process for increased security.

You create login flow screens with the Cloud Flow Designer. Then you embed the screens in the standard Salesforce login page from Setup. During the authentication process, the user is directed to the login flow screens. When users successfully authenticate and complete the login flow, they're redirected to Salesforce. The login process can also log out users immediately if necessary.

When you create a login flow for 2FA, you use Apex methods to get the session context, extract the user's IP address, and verify that the request is coming from a trusted IP range. If the request is coming from within a trusted IP range address, Salesforce skips the flow and logs the user in to the org. If the request is outside the IP range, Salesforce invokes the flow to:

- Direct the user to log in with additional credentials, such as a time-based one-time password (TOTP)
- Force the user to log out
- Direct the user to a page with more options

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To open, edit, or create a flow in the Cloud Flow Designer:

- Manage Force.com Flow

Build Your Own Login Flow

Use the following process to build your own login flow.

1. Create a flow using the Cloud Flow Designer and Apex.

   For example, you can design a custom IP-based 2FA flow that requires a second factor of authentication only if the user is logging in from outside of the trusted IP range.

   Note: To find or set the trusted IP range, from Setup, enter `Network Access` in the Quick Find box, then select **Network Access**.

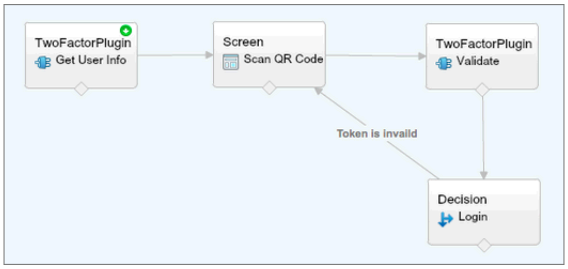
   Note: Don't set login IP ranges directly in a user profile. If you set the IP ranges in a profile, it restricts access for all users of that profile when they're outside the range. Then none of these users can enter the login flow process.

   Include the following in a flow.

   a. A new Apex class for defining an Apex plug-in. The plug-in implements from `Process.Plugin` and uses the `Auth.SessionManagement` class to access the time-based one-time password (TOTP) methods and services. The Apex class for the plug-in generates a time-based key with a quick response (QR) code to validate the TOTP provided by the user against the TOTP generated by Salesforce.

   b. A screen element to scan a QR code.

   c. A decision element to handle when the token is valid and invalid.



Use these input variables to populate the flow at startup.

Name	Value Description
`LoginFlow_LoginType`	Type of login, such as Application, OAuth, or SAML
`LoginFlow_IpAddress`	User's current IP address
`LoginFlow_LoginIpAddress`	User's IP address used during login, which can change after authentication
`LoginFlow_UserAgent`	User agent string provided by the user's browser
`LoginFlow_Platform`	User's operating system
`LoginFlow_Application`	Application used to request authentication
`LoginFlow_Community`	Current community if this login flow applies to a community
`LoginFlow_SessionLevel`	Current session security level, which can be STANDARD or HIGH_ASSURANCE
`LoginFlow_UserId`	User's 18-character ID

Use these variables to specify where the user goes after completing the flow.

Note: You must add a UI screen to the login flow to load these values. The login flow loads these values only after a UI screen is refreshed. A user clicking a button doesn't load the values.

Name	Description
`LoginFlow_FinishLocation`	String. Specify where in the org the user goes after completing the login flow. The string must be a relative path or a valid Salesforce URL. The login process can't redirect the user outside the org.
`LoginFlow_ForceLogout`	Boolean. Set this variable to `true` to log the user out immediately and force the user to exit the login flow.

2. Save the flow.
3. Activate the flow.
4. From the Login Flows Setup page, designate the flow as a login flow and connect it to profiles.

SEE ALSO:

Custom Login Flows

https://developer.salesforce.com/page/Login-Flows

Connect a Login Flow to Profiles

Cloud Flow Designer

Connect a Login Flow to Profiles

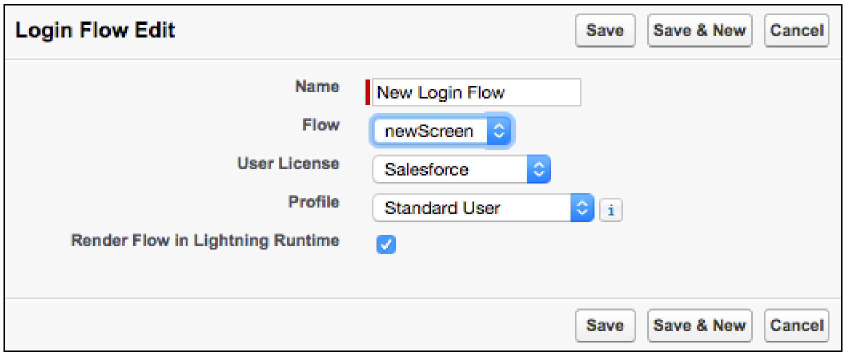
EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

After you create and activate a flow in Cloud Flow Designer, you designate it as a login flow and then associate it with profiles in your org. When users with an associated profile log in, they're directed to this login flow.

1. From Setup, enter *`Login Flows`* in the Quick Find box, then select **Login Flows**.
2. Click **New**.
3. On the Login Flow Edit page, enter a name for the login flow.


Login Flow Edit

Name	New Login Flow
Flow	newScreen
User License	Salesforce
Profile	Standard User
Render Flow in Lightning Runtime	☑

4. Select the login flow from the dropdown list. The list contains flows created with the Cloud Flow Designer. Only active flows of type Flow are supported.
5. Select a user license for the profile that you want to connect to the login flow. When selected, a dropdown list contains the profiles available for the selected license.
6. From the dropdown list, select the profile to associate with the login flow.
7. If you want the login flow to resemble the Lightning Experience UI, select **Render Flow in Lightning Runtime**. If you don't select the option, the login flow resembles Salesforce Classic.

   Note: A login flow is independent of which UI users use: Lightning Experience or Salesforce Classic. You can set a login flow to resemble Lightning Experience even if users log in to Salesforce Classic. Likewise, you can set a login flow to resemble Salesforce Classic even if users log in to Lightning Experience.

8. Click **Save**.

Repeat the process to associate other profiles with the login flow.

After you connect the login flow, you can edit or delete it from the Login Flows Setup page.

SEE ALSO:

Custom Login Flows

Create a Login Flow

Cloud Flow Designer

Set Up Two-Factor Authentication

Admins enable two-factor authentication through permissions or profile settings. Users register devices for two-factor authentication—such as mobile authenticator apps or U2F security keys—through their own personal settings.

You can customize two-factor authentication in the following ways.

- Require it for every login. Set the two-factor login requirement for every time the user logs in to Salesforce. You can also enable this feature for API logins, which includes the use of client applications like the Data Loader. For more information, see Set Two-Factor Authentication Login Requirements or Set Two-Factor Authentication Login Requirements for API Access.
- Use "stepped up" authentication (also known as "high assurance" authentication). Sometimes you don't need two-factor authentication for every user's login, but you want to secure certain resources. If the user tries to use a connected app or reports, Salesforce prompts the user to verify identity. For more information, see Session Security Levels.
- Use profile policies and session settings. First, in the user profile, set the `Session security level required at login` field to **High Assurance**. Then set session security levels in your org's session settings to apply the policy for particular login methods. In your org's session settings, check the session security levels to make sure that Two-Factor Authentication is in the High Assurance column. For more information, see Set Two-Factor Authentication Login Requirements and Custom Policies for Single Sign-On, Social Sign-On, and Communities.

  Warning: If Two-Factor Authentication is in the Standard column, users get an error when they log in with a method that grants standard-level security.

- Use login flows. Use the Flow Designer and profiles to build post-authentication requirements as the user logs in, including custom two-factor authentication processes. For more information, see the following examples.
  - Login Flows

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

- Implementing SMS-Based Two-Factor Authentication
- Enhancing Security with Two-Factor Authentication (Salesforce Classic)

IN THIS SECTION:

Set Two-Factor Authentication Login Requirements

As a Salesforce admin, you can require your users to use a second factor of authentication when they log in.

Set Two-Factor Authentication Login Requirements and Custom Policies for Single Sign-On, Social Sign-On, and Communities

Use profile policies and session settings to set two-factor authentication login requirements for users. All Salesforce user interface authentication methods, including username and password, delegated authentication, SAML single sign-on, and social sign-on through a third-party authentication provider, are supported. You can apply the two-factor authentication requirement to users in Salesforce orgs and Communities.

Set Two-Factor Authentication Login Requirements for API Access

Salesforce admins can set the "Two-Factor Authentication for API Logins" permission to allow using a second authentication challenge for API access to Salesforce. API access includes the use of applications like the Data Loader and developer tools for customizing an organization or building client applications.

Connect Salesforce Authenticator (Version 2 or Later) to Your Account for Identity Verification

The Salesforce Authenticator (version 2 or later) app on your mobile device is the second factor of authentication. Use the app to add an extra level of security to your account.

Verify Your Identity with a One-Time Password Generator App or Device

Connect a one-time password generator app, such as Salesforce Authenticator or Google Authenticator, to verify your identity. The app generates a verification code, sometimes called a "time-based one-time password".

Enable U2F Security Keys for Identity Verification

As a Salesforce admin, you can allow users to use a U2F security key anytime they're challenged to verify their identity, including two-factor authentication and activations. Instead of using Salesforce Authenticator or one-time passwords sent by email or SMS, users insert their U2F security key into a USB port to complete verification.

Register a U2F Security Key for Identity Verification

Register a U2F security key to connect it to your Salesforce account. It's a secure, convenient alternative to using Salesforce Authenticator or one-time passwords sent by email or SMS. Anytime you're challenged to verify your identity, including two-factor authentication and activations, you can insert your security key into a USB port to complete verification.

Disconnect Salesforce Authenticator (Version 2 or Later) from a User's Account

Only one Salesforce Authenticator (version 2 or later) mobile app can be connected to a user's account at a time. If your user loses access to the app by replacing or losing the mobile device, disconnect the app from the user's account. The next time the user logs in with two-factor authentication, if no other authenticator app is connected, Salesforce prompts the user to connect a new authenticator app.

Disconnect a User's One-Time Password Generator App

Besides Salesforce Authenticator, one other mobile authenticator app that generates verification codes (one-time passwords) can be connected to a user's account at a time. If your user loses access to the app by replacing or losing the mobile device, disconnect the app from your user's account. The next time your user logs in with two-factor authentication, if no other identity verification method is connected, Salesforce prompts the user to connect a new authenticator app.

Remove a User's U2F Security Key Registration

One U2F security key can be registered with a user's Salesforce account at a time. If your user replaces or loses a registered security key, remove the registration from your user's account.

Generate a Temporary Identity Verification Code

Generate a temporary verification code for users who can't access the device they usually use for two-factor authentication. You set when the code expires, from 1 to 24 hours after you generate it. The code can be used multiple times until it expires.

Expire a Temporary Verification Code

Expire a user's temporary verification code when the user no longer needs it for two-factor authentication

See How Your Users Are Verifying Their Identity

Customize a list view of users or check the Identity Verification Methods report to find out who's using which methods to verify identity. Create custom reports to spot patterns in identity verification behavior for your org or community.

Delegate Two-Factor Authentication Management Tasks

Let users who aren't Salesforce admins provide support for two-factor authentication in your org. For example, suppose you want your company's Help Desk staff to generate temporary verification codes for users who lost or forgot the device they usually use for two-factor authentication. Assign Help Desk staff members the "Manage Two-Factor Authentication in User Interface" permission so that they can generate codes and support end users with other two-factor authentication tasks.

Set Two-Factor Authentication Login Requirements

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit profiles and permission sets:

- Manage Profiles and Permission Sets

As a Salesforce admin, you can require your users to use a second factor of authentication when they log in.

You can require two-factor authentication each time a user logs in with a username and password to Salesforce, including orgs with custom domains created using My Domain. To set the requirement, select the "Two-Factor Authentication for User Interface Logins" permission in the user profile (for cloned profiles only) or permission set.

See how to set up a two-factor authentication requirement for your org and how your users can use the Salesforce Authenticator app. ▶ Salesforce Authenticator: Set Up a Two-Factor Authentication Requirement (Salesforce Classic)

Users with the "Two-Factor Authentication for User Interface Logins" permission have to provide a second factor, such as a mobile authenticator app or U2F security key, each time they log in to Salesforce.

You can also use a profile-based policy to set a two-factor authentication requirement for users assigned to a particular profile. Use the profile policy when you want to require two-factor authentication for users of the following authentication methods:

- SAML for single sign-on
- Social sign-on in to Salesforce orgs or Communities
- Username and password authentication into Communities

All Salesforce user interface authentication methods, including username and password, delegated authentication, SAML single sign-on, and social sign-on through an authentication provider, are supported. In the user profile, set the `Session security level required at login` field to **High Assurance**. Then set session security levels in your org's session settings to apply the policy for particular login methods. Also in your org's session settings, check the session security levels to make sure that Two-Factor Authentication is in the High Assurance column.

Warning: If Two-Factor Authentication is in the Standard column, users get an error when they log in with a method that grants standard-level security.

SEE ALSO:

Two-Factor Authentication

Set Two-Factor Authentication Login Requirements and Custom Policies for Single Sign-On, Social Sign-On, and Communities

Connect Salesforce Authenticator (Version 2 or Later) to Your Account for Identity Verification

Verify Your Identity with a One-Time Password Generator App or Device

Disconnect Salesforce Authenticator (Version 2 or Later) from a User's Account

Disconnect a User's One-Time Password Generator App

Methods for Verifying Your Identity

Custom Login Flows

Generate a Temporary Identity Verification Code

Expire a Temporary Verification Code

Delegate Two-Factor Authentication Management Tasks

Identity Verification History

Set Two-Factor Authentication Login Requirements and Custom Policies for Single Sign-On, Social Sign-On, and Communities

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit profiles and permission sets:

- Manage Profiles and Permission Sets

To generate a temporary verification code

- Manage Two-Factor Authentication in User Interface

Use profile policies and session settings to set two-factor authentication login requirements for users. All Salesforce user interface authentication methods, including username and password, delegated authentication, SAML single sign-on, and social sign-on through a third-party authentication provider, are supported. You can apply the two-factor authentication requirement to users in Salesforce orgs and Communities.

To require two-factor authentication for users assigned to a particular profile, edit the Session security level required at login profile setting. Then set session security levels in your org's session settings to apply the policy for particular login methods.

By default, the session security requirement at login for all profiles is None. You can edit a profile's Session Settings to change the requirement to High Assurance. When profile users with this requirement use a login method that grants standard-level security instead of high assurance, such as username and password, they're prompted to verify their identity with two-factor authentication. After users authenticate successfully, they're logged in to Salesforce.

You can edit the security level assigned to a login method in your org's Session Settings.

Users with mobile devices can use the Salesforce Authenticator mobile app or another authenticator app for two-factor authentication. Internal users can connect the app to their account in the Advanced User Details page of their personal settings. If you set the High Assurance requirement on a profile, any profile user who doesn't already have Salesforce Authenticator or another authenticator app connected to their account is prompted to connect the app before they can log in. After they connect the app, they're prompted to use the app to verify their identity.

Users with registered U2F security keys can use them for two-factor authentication.

Community members with the High Assurance profile requirement are prompted to connect an authenticator app during login.

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

2. Select a profile.
3. Scroll to Session Settings and find the `Session security level required at login` setting.
4. Click **Edit**.
5. For Session security level required at login, select **High Assurance**.
6. Click **Save**.
7. From Setup, enter *`Session Settings`* in the Quick Find box, then select **Session Settings**.
8. In Session Security Levels, make sure that Two-Factor Authentication is in the High Assurance column.
   If Two-Factor Authentication is in the Standard column, users get an error when they log in with a method that grants standard-level security.
9. Note: Consider moving Activation to the High Assurance column. With this setting, users who verify their identity from an unrecognized browser or app establish a high-assurance session. When Activation is in the High Assurance column, profile users who verify their identity at login aren’t challenged to verify their identity again to satisfy the high-assurance session security requirement.

   Save your changes.

Example: You’ve configured Facebook and LinkedIn as authentication providers in your community. Many of your community members use social sign-on to log in using the username and password from their Facebook or LinkedIn accounts. You want to increase security by requiring Customer Community users to use two-factor authentication when they log in with their Facebook account, but not with their LinkedIn account. You edit the Customer Community User profile and set the Session security level required at login to **High Assurance**. In your org’s Session Settings, you edit the Session Security Levels. You place Facebook in the Standard column. In the High Assurance column, you place Two-Factor Authentication. You also place LinkedIn in the High Assurance column.

Note: You can also use login flows to change the user’s session security level to initiate identity verification under specific conditions. Login flows let you build a custom post-authentication process that meets your business requirements.

If users lose or forget the device they usually use for two-factor authentication, you can generate a temporary verification code for them. You set when the code expires, from 1 to 24 hours after you generate it. Your user can use the code multiple times until it expires. A user can have only one temporary code at a time. If a user needs a new code while the old code is still valid, you can expire the old code, then generate a new one. Users can expire their own valid codes in their personal settings.

Note: The `High Assurance` profile requirement applies to user interface logins. OAuth token exchanges aren’t subject to the requirement. OAuth refresh tokens that were obtained before a `High Assurance` requirement is set for a profile can still be exchanged for access tokens that are valid for the API. Tokens are valid even if they were obtained with a standard-assurance session. To require users to establish a high-assurance session before accessing the API with an external application, first revoke existing OAuth tokens for users with that profile. Then set a `High Assurance` requirement for the profile. Users have to log in with two-factor authentication and reauthorize the application.

SEE ALSO:

- Two-Factor Authentication
- Custom Login Flows
- Connect Salesforce Authenticator (Version 2 or Later) to Your Account for Identity Verification
- Verify Your Identity with a One-Time Password Generator App or Device
- Disconnect Salesforce Authenticator (Version 2 or Later) from a User's Account
- Disconnect a User's One-Time Password Generator App
- Generate a Temporary Identity Verification Code
- Expire a Temporary Verification Code
- Delegate Two-Factor Authentication Management Tasks
- Expire a Temporary Verification Code

Set Two-Factor Authentication Login Requirements for API Access

Salesforce admins can set the "Two-Factor Authentication for API Logins" permission to allow using a second authentication challenge for API access to Salesforce. API access includes the use of applications like the Data Loader and developer tools for customizing an organization or building client applications.

The "Two-Factor Authentication for User Interface Logins" permission is a prerequisite for the "Two-Factor Authentication for API Logins" permission. Users who have these permissions enabled have to complete two-factor authentication when they log in to Salesforce through the user interface. Users must download and install an authenticator app on their mobile device and connect the app to their Salesforce account. Then they can use verification codes (time-based one-time passwords, or TOTP) from the app for two-factor authentication.

SEE ALSO:

- Two-Factor Authentication
- Verify Your Identity with a One-Time Password Generator App or Device
- Set Two-Factor Authentication Login Requirements
- Reset Your Security Token
- Identity Verification History

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit system permissions in profiles:

- Manage Profiles and Permission Sets

To enable this feature:

- Two-Factor Authentication for User Interface Logins

Connect Salesforce Authenticator (Version 2 or Later) to Your Account for Identity Verification

EDITIONS

Salesforce Authenticator setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Essentials**, **Group**, **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Contact Manager** Editions

The Salesforce Authenticator (version 2 or later) app on your mobile device is the second factor of authentication. Use the app to add an extra level of security to your account.

1. Download and install version 2 or later of the Salesforce Authenticator app for the type of mobile device you use. For iPhone, get the app from the App Store. For Android devices, get the app from Google Play.

   If you previously installed version 1 of Salesforce Authenticator on your mobile device, you can update the app to version 2 through the App Store or Google Play. The update preserves any connected accounts you already have in the app. These accounts are code-only accounts that generate verification codes but don't receive push notifications or allow location-based automated verifications. If you have a code-only account for the username you used for your current login to Salesforce, swipe left in the app to remove that username before proceeding. In the following steps, you connect the account for that username again. The new connected account gives you full Salesforce Authenticator version 2 functionality: push notifications, location-based automated verifications, and verification codes.

2. From your personal settings, enter *Advanced User Details* in the `Quick Find` box, then select **Advanced User Details**. No results? Enter *Personal Information* in the `Quick Find` box, then select **Personal Information**.
3. Find **App Registration: Salesforce Authenticator** and click **Connect**.
4. For security purposes, you're prompted to log in to your account.
5. Open the Salesforce Authenticator app on your mobile device.

   If you're opening the app for the first time, you see a tour of the app's features. Take the tour, or go straight to adding your Salesforce account to the app.

6. In the app, tap **+** to add your account.

   The app generates a unique two-word phrase.

7. Back in your browser, enter the phrase in the `Two-Word Phrase` field.
8. Click **Connect**.

   If you previously connected an authenticator app that generates verification codes to your account, you sometimes see an alert. Connecting version 2 or later of the Salesforce Authenticator mobile app invalidates the codes from your old app. When you need a verification code, get it from Salesforce Authenticator from now on.

9. In the Salesforce Authenticator app on your mobile device, you see details about the account you're connecting. To complete the account connection, tap **Connect** in the app.

To help keep your account secure, we send you an email notification whenever a new identity verification method is added to your Salesforce account. You get the email whether you add the method or your Salesforce admin adds it on your behalf.

If your administrator requires two-factor authentication for increased security when you log in or access reports or dashboards, use the app to verify your account activity. If you're required to use two-factor authentication before you have the app connected, you're prompted to connect it the next time you log in to Salesforce. If you don't yet have the two-factor authentication requirement, you can still connect the app to your account through your personal settings.

After you connect the app, you get a notification on your mobile device when you do something that requires identity verification. When you receive the notification, open the app on your mobile device, check the activity details, and respond on your mobile device to verify. If you are notified about activity you don't recognize, use the app to block the activity. You can flag the blocked activity for your Salesforce admin. The app also provides a verification code that you can use as an alternate method of identity verification.

Verify Your Identity with a One-Time Password Generator App or Device

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

Available in all editions

Connect a one-time password generator app, such as Salesforce Authenticator or Google Authenticator, to verify your identity. The app generates a verification code, sometimes called a "time-based one-time password".

If your company requires two-factor authentication for increased security when you log in, access connected apps, reports, or dashboards, use a code from the app. If you're required to use two-factor authentication before you have an app connected, you're prompted to connect one the next time you log in to Salesforce.

1. Download the supported authenticator app for your device type. You can use any authenticator app that supports the time-based one-time password (TOTP) algorithm (IETF RFC 6238), such as Salesforce Authenticator for iOS, Salesforce Authenticator for Android, or Google Authenticator.
2. From your personal settings, enter *Advanced User Details* in the `Quick Find` box, then select **Advanced User Details**. No results? Enter *Personal Information* in the `Quick Find` box, then select **Personal Information**.
3. Find `App Registration: One-Time Password Generator` and click **Connect**.

   If you're connecting an authenticator app other than Salesforce Authenticator, use this setting. If you're connecting Salesforce Authenticator, use this setting if you're only using its one-time password generator feature (not the push notifications available in version 2 or later).

   Note: If you're connecting Salesforce Authenticator so that you can use push notifications, use the `App Registration: Salesforce Authenticator` setting instead. That setting enables both push notifications and one-time password generation.

   You can connect up to two authenticator apps to your Salesforce account for one-time password generation: Salesforce Authenticator and one other authenticator app.
4. For security purposes, you're prompted to log in to your account.
5. Using the authenticator app on your mobile device, scan the QR code.

   Alternatively, click **I Can't Scan the QR Code** in your browser. The browser displays a security key. In the authenticator app, enter your username and the key displayed.
6. In Salesforce, enter the code generated by the authenticator app in the `Verification Code` field.

   The authenticator app generates a new verification code periodically. Enter the current code.
7. Click **Connect**.

To help keep your account secure, we send you an email notification whenever a new identity verification method is added to your Salesforce account. You get the email whether you add the method or your Salesforce admin adds it on your behalf.

Enable U2F Security Keys for Identity Verification

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To enable U2F security keys:

- Customize Application

  AND

  Manage Users

As a Salesforce admin, you can allow users to use a U2F security key anytime they're challenged to verify their identity, including two-factor authentication and activations. Instead of using Salesforce Authenticator or one-time passwords sent by email or SMS, users insert their U2F security key into a USB port to complete verification.

The Universal Second Factor (U2F) authentication standard is part of the FIDO Alliance and features the security of public-key cryptography, which strongly resists phishing. U2F security keys, which commonly plug into a USB port, are easy to deploy and work well in environments where mobile devices aren't allowed. Users can use the same security key with multiple service providers and multiple Salesforce orgs and accounts.

It's worth mentioning a few things about how security keys work.

- Users can self-provision their own security keys. These devices don't require upfront registration by IT or admins.
- Security keys can look similar to other USB authentication devices that users carry on a keychain. Try to look for the FIDO U2F logo indicating that the device is compatible with the U2F protocol. If you're not sure, verify with your security hardware vendor that their keys are U2F compliant.
- Security keys aren't a biometric device, even though some have a button that requires the user's touch to activate the device. After the user inserts and activates the security key, it generates the required credentials, and the browser passes them on to Salesforce to complete the login.
- For now, this identity verification method is supported only in Chrome version 41 or later because it's the only browser that natively supports U2F.

After you enable U2F security keys in your org, any user can individually register a security key to connect the device to their Salesforce account. Then they can use it for identity verification.

1. From Setup, enter *`Session Settings`* in the `Quick Find` box, then select **Session Settings**.
2. Select `Let users use a security key`.

   Important: My Domain must be enabled before you enable U2F security keys. If your org has deployed My Domain, you have access to this setting.

3. Save your changes.

As with other identity verification methods, you can use standard tools in Salesforce to track users' security key usage.

- View users' security key activity on the Identity Verification History page.
- Monitor security key adoption using the Identity Verification Methods report (via the link on the Identity Verification History page).
- Create user list views that include the `Has U2F Security Key` field to see who has registered this method.

Using the Mass Email Users tool, you can send targeted communications to users who have registered this method.

Register a U2F Security Key for Identity Verification

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

Register a U2F security key to connect it to your Salesforce account. It's a secure, convenient alternative to using Salesforce Authenticator or one-time passwords sent by email or SMS. Anytime you're challenged to verify your identity, including two-factor authentication and activations, you can insert your security key into a USB port to complete verification.

If your Salesforce admin has allowed the use of U2F security keys, register your own security key (an admin can't register for you). Keep in mind these considerations.

- Make sure that your security key is compatible with the U2F protocol. Security keys can look similar to other USB authentication devices that fit on a keychain. Try to look for the FIDO U2F logo indicating that the device is U2F compliant. If you're not sure, verify with your Salesforce admin.
- Make sure that your browser is compatible. For now, Google Chrome version 41 or later is the only browser that natively supports U2F. All registration and identity verification activity is supported only in Chrome version 41 or later.
- You can use the same security key with multiple service providers and multiple Salesforce orgs and accounts. You can register one key per account.

1. Have your U2F-compliant security key in hand so that you're ready to insert it when prompted. If you wait too long, your registration attempt can time out.
2. From your personal settings, enter `Advanced User Details` in the `Quick Find` box, then select **Advanced User Details**. No results? Enter `Personal Information` in the `Quick Find` box, then select **Personal Information**.
3. Click **Register** next to the `Security Key (U2F)` field.

   If you don't see this option, your Salesforce admin has disallowed the use of security keys.
4. For security purposes, you're prompted to log in to your account.
5. At the prompt, insert your security key into your computer's USB port. If it has a button, touch the button.

   Security keys aren't a biometric device, even though some have a button that requires your touch to activate the device.
6. After successful registration, click **Continue** to dismiss the confirmation message.

   To help keep your account secure, we send you an email notification after successful registration.

Now you're ready to use this identity verification method. When we prompt you for your U2F security key, insert it and touch the button if it has a button. The security key generates the required credentials, and the browser passes them on to Salesforce to complete the verification.

If you're ever without your security key, you can still use other verification methods, such as Salesforce Authenticator or another method that generates a verification code. If you need a temporary alternate method for two-factor authentication, your admin can generate a temporary verification code (not available for activations).

You can cancel your security key registration at any time, and so can an admin.

Disconnect Salesforce Authenticator (Version 2 or Later) from a User's Account

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To disconnect a user's Salesforce Authenticator app:

- Manage Two-Factor Authentication in User Interface

Only one Salesforce Authenticator (version 2 or later) mobile app can be connected to a user's account at a time. If your user loses access to the app by replacing or losing the mobile device, disconnect the app from the user's account. The next time the user logs in with two-factor authentication, if no other authenticator app is connected, Salesforce prompts the user to connect a new authenticator app.

1. From Setup, enter *`Users`* in the `Quick Find` box, then select **Users**.
2. Click the user's name.
3. On the user's detail page, click **Disconnect** next to the `App Registration: Salesforce Authenticator` field.

Users can disconnect the app from their own account on the Advanced User Details page. In personal settings, the user clicks **Disconnect** next to the `App Registration: Salesforce Authenticator` field.

Disconnect a User's One-Time Password Generator App

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To disconnect a user's authenticator app:

- Manage Two-Factor Authentication in User Interface

Besides Salesforce Authenticator, one other mobile authenticator app that generates verification codes (one-time passwords) can be connected to a user's account at a time. If your user loses access to the app by replacing or losing the mobile device, disconnect the app from your user's account. The next time your user logs in with two-factor authentication, if no other identity verification method is connected, Salesforce prompts the user to connect a new authenticator app.

1. From Setup, enter *`Users`* in the `Quick Find` box, then select **Users**.
2. Click the user's name.
3. On the user's detail page, click **Disconnect** next to the `App Registration: One-Time Password Generator` field.

Your users can disconnect the app from their own account. In personal settings, they go to the Advanced User Details page and click **Disconnect** next to the `App Registration: One-Time Password Generator` field.

SEE ALSO:

View and Manage Users

Delegate Two-Factor Authentication Management Tasks

Update Personal Information

Remove a User's U2F Security Key Registration

One U2F security key can be registered with a user's Salesforce account at a time. If your user replaces or loses a registered security key, remove the registration from your user's account.

1. From Setup, enter *Users* in the `Quick Find` box, then select **Users**.
2. Click the user's name.
3. On the user's detail page, click **Remove** next to the `Security Key (U2F)` field.

Your users can remove a registered security key from their own account. In personal settings, they go to the Advanced User Details page and click **Remove** next to the `Security Key (U2F)` field.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To remove a user's U2F security key registration:

- Manage Two-Factor Authentication in User Interface

Generate a Temporary Identity Verification Code

Generate a temporary verification code for users who can't access the device they usually use for two-factor authentication. You set when the code expires, from 1 to 24 hours after you generate it. The code can be used multiple times until it expires.

Temporary verification codes are valid for two-factor authentication only. They aren't valid for device activations. That is, when users log in from an unrecognized browser or app and we require identity verification, they can't use a temporary code.

1. From Setup, enter *Users* in the `Quick Find` box, then select **Users**.
2. Click the name of the user who needs a temporary verification code.

   You can't generate a code for an inactive user.
3. Find `Temporary Verification Code`, then click **Generate**.

   If you don't already have a session with a high-assurance security level, Salesforce prompts you to verify your identity.
4. Set when the code expires, and click **Generate Code**.
5. Give the code to your user, then click **Done**.

   After you click **Done**, you can't return to view the code again, and the code isn't displayed anywhere in the user interface.

Your user can use the temporary verification code multiple times until it expires. Each user can have only one temporary verification code at a time. If a user forgets or loses the code before it expires, you can manually expire the old code and generate a new one. You can generate up to six codes per hour for each user.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To generate a temporary verification code:

- Manage Two-Factor Authentication in User Interface

Note: When you add an identity verification method to a user's account, the user gets an email. To stop sending emails to users when new identity verification methods are added to their accounts, contact Salesforce.

SEE ALSO:

- Two-Factor Authentication
- Delegate Two-Factor Authentication Management Tasks
- Expire a Temporary Verification Code

Expire a Temporary Verification Code

Expire a user's temporary verification code when the user no longer needs it for two-factor authentication

Each user can have only one temporary verification code at a time. If a user forgets or loses the code before it expires, you can manually expire the old code and generate a new one. You can generate up to six codes per hour for each user.

1. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.
2. Click the name of the user whose temporary verification code you need to expire.
3. Find `Temporary Verification Code`, and click **Expire Now**.

SEE ALSO:

- Two-Factor Authentication
- Delegate Two-Factor Authentication Management Tasks
- Generate a Temporary Identity Verification Code

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To expire a user's temporary verification code:

- Manage Two-Factor Authentication in User Interface

See How Your Users Are Verifying Their Identity

Customize a list view of users or check the Identity Verification Methods report to find out who's using which methods to verify identity. Create custom reports to spot patterns in identity verification behavior for your org or community.

To see registered identity verification methods in a Users list view, create or edit a view and add one or more of the following fields.

Has Verified Mobile Number

Indicates whether the user has verified a mobile phone number. Salesforce can text a verification code to the user at that number.

Has One-Time Password App

Indicates whether the user has connected an authenticator app that generates verification codes, also known as time-based one-time passwords. The user can verify identity by entering a code generated by the app.

Has Salesforce Authenticator

Indicates whether the user has connected the Salesforce Authenticator mobile app. The user can verify identity by approving a notification sent to the app.

EDITIONS

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

USER PERMISSIONS

To monitor user identity verification methods:

- Manage Two-Factor Authentication in User Interface

Has Temporary Code

Indicates whether the user has a temporary verification code. Admins or non-admin users with the "Manage Two-Factor Authentication in User Interface" permission generate temporary codes and set when the code expires.

Has U2F Security Key

Indicates whether the user has registered a U2F security key. The user can verify identity by inserting the security key into a USB port.

You can perform some two-factor authentication support tasks right in the list view. For example, you can generate or expire a temporary verification code or disconnect a mobile authenticator app when the user loses access to the mobile device.

To view and customize the Identity Verification Methods report, users with the "Manage Two-Factor Authentication in User Interface" permission can click the link on the Identity Verification History page in Setup.

Users with the "View Setup and Configuration" permission can also access the report from the Administrative Reports folder in Reports.

Users with the "Manage Two-Factor Authentication in API" permission can create custom reports and dashboards for even deeper insight into identity verification history in your org or community. For example, create a report that shows identity verification method registration by profile. Or create a dashboard with charts that show method registration and verification challenges by the org policy that triggered them.

SEE ALSO:

Two-Factor Authentication

Delegate Two-Factor Authentication Management Tasks

Delegate Two-Factor Authentication Management Tasks

Let users who aren't Salesforce admins provide support for two-factor authentication in your org. For example, suppose you want your company's Help Desk staff to generate temporary verification codes for users who lost or forgot the device they usually use for two-factor authentication. Assign Help Desk staff members the "Manage Two-Factor Authentication in User Interface" permission so that they can generate codes and support end users with other two-factor authentication tasks.

To assign the permission, select "Manage Two-Factor Authentication in User Interface" in the user profile (for cloned profiles only) or permission set. Users with the permission can perform the following tasks.

- Generate a temporary verification code for a user who can't access the device normally used for two-factor authentication.
- Disconnect identity verification methods from a user's account when the user loses or replaces a device.
- View user identity verification activity on the Identity Verification History page.
- View the Identity Verification Methods report by clicking a link on the Identity Verification History page.
- Create user list views that show which identity verification methods users have registered.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit profiles and permission sets:

- Manage Profiles and Permission Sets

Note: Although non-admin users with the permission can view the Identity Verification Methods report, they can't create custom reports that include data restricted to users with the "Manage Users" permission.

SEE ALSO:

- Protect Your Salesforce Organization
- Disconnect Salesforce Authenticator (Version 2 or Later) from a User's Account
- Disconnect a User's One-Time Password Generator App
- Generate a Temporary Identity Verification Code
- Expire a Temporary Verification Code
- See How Your Users Are Verifying Their Identity

Transaction Security

Transaction Security is a framework that intercepts real-time Salesforce events and applies appropriate actions and notifications based on security policies you create. Transaction Security monitors events according to the policies that you set up. These policies are applied against events in your org and specify actions to take when certain event combinations occur. When a policy is triggered, you can have an action taken and receive an optional notification.

EDITIONS

Available in: Lightning Experience

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

Requires purchasing Salesforce Shield or Salesforce Shield Event Monitoring add-on subscriptions.

IN THIS SECTION:

Transaction Security Policies

Policies evaluate activity using events that you specify. For each policy, you define real-time actions, such as notify, block, force two-factor authentication, freeze user, or end a session.

Transaction Security Metering

Transaction Security uses resource metering to help prevent malicious or unintentional monopolization of shared, multitenant platform resources. Metering prevents policy evaluations from using too many resources and impacting your org.

Set Up Transaction Security

Activate and configure transaction security on your org before creating your own custom policies. Only an active user assigned the System Administrator profile can use this feature.

Create Custom Transaction Security Policies

Create your own custom policies, triggered by specific events. Only an active user assigned the System Administrator profile can use this feature.

Create Transaction Security Policies with Salesforce Classic

Create a policy in Salesforce Classic using a single form, including a basic Apex event class.

Create Transaction Security Policies with Lightning Experience

Let the Transaction Security wizard walk you through the steps to create a policy.

Apex Policies for Transaction Security Notifications

Every Transaction Security policy must implement the Apex `TxnSecurity.PolicyCondition` interface. Here are several examples.

Manage Transaction Security Policies

Use Transaction Security policies to define, enable, and generate Apex code to implement your policies. Specify how to be notified when a policy is triggered, and then select the policies to enable. Only an active user assigned the System Administrator profile can use this feature.

Receiving Transaction Security Notifications

You receive the notifications you've selected when an enabled policy is triggered. The notifications are formatted for easy recognition.

Transaction Security Policies

Policies evaluate activity using events that you specify. For each policy, you define real-time actions, such as notify, block, force two-factor authentication, freeze user, or end a session.

When you enable Transaction Security for your org, two policies are created:

- Concurrent User Session Limit policy to limit concurrent login sessions
- Lead Data Export policy to block excessive data downloads of leads

The policies' corresponding Apex classes are also created in the org. An administrator can enable the policies immediately or edit their Apex classes to customize them.

For example, suppose that you activate the Concurrent User Session Limit policy to limit the number of concurrent sessions per user. In addition, you change the policy to notify you via email when the policy is triggered. You also update the policy's Apex implementation to limit users to three sessions instead of the default five sessions. (That's easier than it sounds.) Later, someone with three login sessions tries to create a fourth. The policy prevents that and requires ending one of the existing sessions before proceeding with the new session. At the same time, you are notified that the policy was triggered.

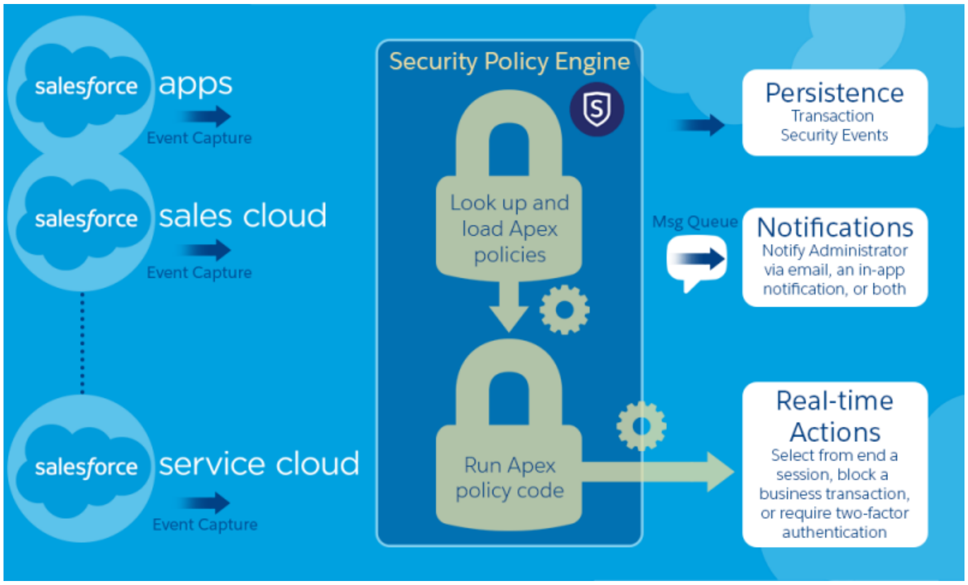
EDITIONS

Available in: Lightning Experience

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

Requires purchasing Salesforce Shield or Salesforce Shield Event Monitoring add-on subscriptions.

The Transaction Security architecture uses the Security Policy Engine to analyze events and determine the necessary actions.


salesforce
apps
Event Capture
salesforce
sales cloud
Event Capture
salesforce
service cloud
Event Capture
Security Policy Engine
Look up and load Apex policies
Run Apex policy code
Msg Queue
Persistence
Transaction Security Events
Notifications
Notify Administrator via email, an in-app notification, or both
Real-time Actions
Select from end a session, block a business transaction, or require two-factor authentication

A transaction security policy consists of events, notifications, and actions.

- Available event types are:
  - Data Export for Account, Case, Contact, Lead, and Opportunity objects
  - Entity for authentication providers and sessions, client browsers, login IP, and Chatter resources

  - Logins
  - Resource Access for connected apps and reports and dashboards
- You can be notified via email, by an in-app notification, or both.
- Actions to take if the policy is triggered:
  - Block the operation
  - Require a higher level of assurance using two-factor authentication
  - Freeze the user
  - End a current session

  You can also take no action and only receive a notification. The actions available depend on the event type and resource selected.

Transaction Security Metering

Transaction Security uses resource metering to help prevent malicious or unintentional monopolization of shared, multitenant platform resources. Metering prevents policy evaluations from using too many resources and impacting your org.

Policies are metered for uniform resource use. If a policy request can’t be handled quickly enough, a fail-close behavior occurs, and access is blocked. Transaction Security implements metering by limiting policy execution. If the elapsed execution time exceeds three seconds, the user is denied access to the resource or entity.

Here’s an example of how metering works for login policies. Your org has a login policy with a notification action. A user makes four login requests concurrently, but they can’t all be executed in sufficient time. Transaction Security stops processing the policies and fails closed, blocking all four login requests. Because the policy evaluations didn’t finish, a notification isn’t sent.

EDITIONS

Available in: Lightning Experience

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

Requires purchasing Salesforce Shield or Salesforce Shield Event Monitoring add-on subscriptions.

Set Up Transaction Security

Activate and configure transaction security on your org before creating your own custom policies. Only an active user assigned the System Administrator profile can use this feature.

EDITIONS

Available in: Lightning Experience

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

Requires purchasing Salesforce Shield or Salesforce Shield Event Monitoring add-on subscriptions.

USER PERMISSIONS

User Permissions Needed
To create, edit, and manage transaction security policies: - Customize Application
To manage transaction security policies: - Author Apex

1. Enable transaction security policies to make them available for use.
   a. From Setup, enter `Transaction Security` in the `Quick Find` box, then select **Transaction Security**.
   b. Select **Enable custom transaction security policies** at the top of the page.

   The ConcurrentSessionsLimitingPolicy limits concurrent sessions and is triggered in two ways:

   - When a user with five current sessions tries to log in for a sixth session
   - When an administrator that's already logged in tries to log in a second time

   You can adjust the number of sessions allowed by changing the Apex policy implementation `ConcurrentSessionsPolicyCondition`.

   The Lead Data Export policy blocks excessive data downloads of leads. It's triggered when a download either:

   - Retrieves more than 2,000 lead records
   - Takes more than one second to complete

   You can change these values by modifying the `DataLoaderLeadExportCondition` policy implementation.

2. After Transaction Security is enabled, set the preferences for your org.
   a. Click **Default Preferences** on the Transaction Security Policies page.
   b. Select the preference **When users exceed the maximum number of Salesforce sessions allowed, close the oldest session.**

   Login policies affect programmatic access and access from Salesforce Classic and Lightning Experience. When you create a policy that limits the number of concurrent user sessions, all sessions count toward that limit. Regular logins with a username and password, logins by web applications, logins using Authentication Providers, and all other login types are considered.

   The session limit isn't a problem in Salesforce Classic or Lightning Experience because you're prompted to select which session or sessions to end. That choice isn't available from within a program, so the program receives a Transaction Security exception that the session limit has been reached.

   To prevent this problem, select **When users exceed the maximum number of Salesforce sessions allowed, close the oldest session.**. Then when a programmatic request is made that exceeds the number of sessions allowed, older sessions are ended until the session count is below the limit. The setting also works for logins from the UI. Instead of being asked to select a session to end, the oldest session is automatically ended, and the new login proceeds for the new session. Here's how the OAuth flows handle login policies with and without the preference being set.

Flow Type	Action If Preference Is Selected	Action If Preference Is Not Selected
OAuth 2.0 web server	Authorization Code and Access Token granted Older sessions are ended until you're within policy compliance.	Authorization Code granted, but Access Token not granted Older sessions are ended until you're within policy compliance.

Flow Type	Action If Preference Is Selected	Action If Preference Is Not Selected
OAuth 2.0 user-agent	Access Token granted Older sessions are ended until you're within policy compliance.	Access Token granted Older sessions are ended until you're within policy compliance.
OAuth 2.0 refresh token flow	Access Token granted Older sessions are ended until you're within policy compliance.	TXN_SECURITY_END_SESSION exception
OAuth 2.0 JWT bearer token	Access Token granted Older sessions are ended until you're within policy compliance.	TXN_SECURITY_END_SESSION exception
OAuth 2.0 SAML bearer assertion	Access granted Older sessions are ended until you're within policy compliance.	TXN_SECURITY_END_SESSION exception
OAuth 2.0 username and password	Access granted Older sessions are ended until you're within policy compliance.	Access denied due to more than the number of sessions allowed by the policy
SAML assertion	Not applicable	Not applicable

For more information on authentication flows, see Authenticate Apps with OAuth in the Salesforce help.

Create Custom Transaction Security Policies

Create your own custom policies, triggered by specific events. Only an active user assigned the System Administrator profile can use this feature.

The way you create a policy depends on which UI you're using.

- If you're using Salesforce Classic, refer to Create Transaction Security Policies with Salesforce Classic.
- If you're using Lightning Experience, refer to Create Transaction Security Policies with Lightning Experience.

You can create multiple policies for the same type of event, but we recommend that your policies and their actions don't overlap. All the policies for a given event execute when the event occurs, but their order of execution is indeterminate. For example, if you have two policies enabled for an exported contact, you can't be sure which policy is triggered first. If one policy copies the contact and the other policy deletes the contact, the copy operation fails if the deletion is done first.

EDITIONS

Available in: Lightning Experience

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

Requires purchasing Salesforce Shield or Salesforce Shield Event Monitoring add-on subscriptions.

USER PERMISSIONS

User Permissions Needed
To create, edit, and manage transaction security policies: • Customize Application
To manage transaction security policies: • Author Apex

Create Transaction Security Policies with Salesforce Classic

Create a policy in Salesforce Classic using a single form, including a basic Apex event class.

EDITIONS

Available in: Lightning Experience

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

Requires purchasing Salesforce Shield or Salesforce Shield Event Monitoring add-on subscriptions.

USER PERMISSIONS

User Permissions Needed
To create, edit, and manage transaction security policies: • Customize Application
To manage transaction security policies: • Author Apex

1. From Setup, enter `Transaction Security` in the `Quick Find` box, select **Transaction Security**, and then click **New** in Transaction Security Policies.
2. Enter the basic information fields for your new policy.
   - For clarity and easier maintenance, use similar names for the API and the policy. 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.
   - `Event Type`—Determines the available actions. It can be one of the following:
     - **Login**—A user login. Login lets you set any combination of notifications, plus these actions:
       - Block access completely
       - Continue, but require two-factor authentication
       - Continue, but require the end of a current login session
     - **Entity**—An object type. Select a specific resource and the type of notifications desired. The Freeze User action is available for Chatter resources.
     - **Data Export**—Notifies you when the selected object type has been exported. Available object types are Account, Case, Contact, Lead, and Opportunity. To trigger a policy, the export must be done using a default report type from the Report tab or with an API client like Data Loader or Workbench.

       Note: You can't create a Data Export event policy for joined reports, historical reports, or custom report types.
     - **AccessResource**—Notifies you when the selected resource has been accessed. You can block access or require two-factor authentication before access is allowed.
   - `Notifications`—You can select all, some, or no notification methods for each policy.
   - `Recipient`—Must be an active user assigned the System Administrator profile.
   - `Real-time Actions`—Specifies what to do when the policy is triggered. The actions available vary depending on the event type. For login and resource events, you can also block the action or require a higher level of access control with two-factor authentication. For Chatter events, you can freeze the user or block the post. For Login events, you can require ending an existing session before continuing with the current session. You can set the default action for ending a session to always close the oldest session.

     Important: If you create a policy requiring the two-factor authentication action, provide your users a way to get a time-based, one-time password. This password is their second authentication factor. Otherwise, if your users encounter a situation that requires a second authentication factor, they can't finish their task, such as logging in or running a report.
   - You can use an existing class for `Apex Policy` or select **Generate Apex** to have a default policy class created that implements the `TxnSecurity.PolicyCondition` interface. You can also write your own policy to take advantage of any customizations you've made to your org.
   - The user selected for `Execute Policy As` must have the System Administrator profile.
3. You can optionally create a condition for a specific property as part of the policy. For example, you can create a policy that's triggered when a report or dashboard is accessed from a specific source IP. The source IP is the property you're checking.

- The available properties depend on the event type selected.
- For example, with Login events, property changes that occurred within a given number of days or an exact match to a property value are available.

4. To enable a policy, select the policy's checkbox. You can enable and disable policies according to your requirements.
5. Click **Save**.

After saving your selection, you're shown the editing page for your new policy. You can modify your policy here and review its Apex class.

If you didn't specify a condition value before you generated the Apex interface for a policy, you can add the condition later. If you want to change the condition, you can edit it. Edit the Apex code to include a condition before you activate your policy. If you never include a condition, your policy is never triggered. See Apex Policies for Transaction Security Notifications for examples.

Create Transaction Security Policies with Lightning Experience

Let the Transaction Security wizard walk you through the steps to create a policy.

1. From Setup, enter *Transaction* in the `Quick Find` box, select **Transaction Security**, and then click **Create Policy** in Transaction Security Policies.
2. First select what your policy monitors. Choose a category and then select an event or entity in that category.

   The categories are:

   - **Data Export**—Notifies you when the selected object type has been exported. To trigger a policy, the export must be done using a default report type from the Report tab or with an API client like Data Loader or Workbench.

     Note: You can't create a Data Export event policy for joined reports, historical reports, or custom report types.

   - **Login**—A user login. You can trigger your policy on many types of login events.
   - **Resource Access**—Notifies you when the selected resource has been accessed. You can block access or require two-factor authentication before access is allowed.
   - **Entity**—An object type.

     Note: Lightning Experience supports only the Feed Comment and Feed Item resources, while Salesforce Classic supports all Chatter resources.

3. Select Generate Apex unless you have an existing policy condition to use.

   Transaction Security creates a stub, or placeholder, Apex policy condition. You'll expand it after creating the policy.

4. Next select what the policy is to do when triggered, who is to be notified and how, and the user that the policy executes as. The user selected for `Execute Policy As` must have the System Administrator profile.

   The actions available vary depending on the event type. For login and resource events, you can also block the action or require a higher level of access control with two-factor authentication. For Chatter events, you can freeze the user or block the post. For Login events, you can require ending an existing session before continuing with the current session. You can set the default action for ending a session to always close the oldest session.

   Note: Two-factor authentication is not available in the Salesforce app or Lightning Experience for the Resource Access event type. The Block action is used instead.

EDITIONS

Available in: Lightning Experience

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

Requires purchasing Salesforce Shield or Salesforce Shield Event Monitoring add-on subscriptions.

USER PERMISSIONS

User Permissions Needed

To create, edit, and manage transaction security policies:
- Customize Application

To manage transaction security policies:
- Author Apex

Important: If you create a policy requiring the two-factor authentication action, provide your users a way to get a time-based, one-time password. This password is their second authentication factor. Otherwise, if your users encounter a situation that requires a second authentication factor, they can't finish their task, such as logging in or running a report.

5. Choose a descriptive name for your policy. The name and policy description help you identify and organize policies as they are created.
6. Click **Save** and then click **Finish** to confirm. The new policy appears at the bottom of the policy list.

If you didn't select an existing Apex class for your new policy, modify the generated Apex class now, before activating your policy. Click the Apex class name to get started and add the condition that triggers the policy. See Apex Policies for Transaction Security Notifications for examples.

Apex Policies for Transaction Security Notifications

Every Transaction Security policy must implement the Apex `TxnSecurity.PolicyCondition` interface. Here are several examples.

If you didn't specify a condition value before you generated the Apex interface for a policy, you can add the condition later. If you want to change the condition, you can edit it. Edit the Apex code to include a condition before you activate your policy. If you never include a condition, your policy is never triggered. See the following examples for how to write up the condition.

Don't include Data Manipulation Language (DML) statements in your custom policies. DML operations are rolled back after a transaction security policy is evaluated, regardless if the policy evaluates to `true` or `false`.

When you delete a transaction security policy, your `TxnSecurity.PolicyCondition` implementation isn't deleted. You can reuse your Apex code in other policies.

This Apex policy example implements a policy that is triggered when someone logs in from multiple IP addresses in the past 24 hours.

EDITIONS

Available in: Lightning Experience

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

Requires purchasing Salesforce Shield or Salesforce Shield Event Monitoring add-on subscriptions.

Example:

```
global class LoginPolicyCondition implements TxnSecurity.PolicyCondition {
  public boolean evaluate(TxnSecurity.Event e) {
    AggregateResult[] results = [SELECT SourceIp
                                 FROM LoginHistory
                                 WHERE UserId = :e.userId
                                       AND LoginTime = LAST_N_DAYS:1
                                 GROUP BY SourceIp];
    if(!results.isEmpty() && results.size() > 1) {
      return true;
    }
    return false;
  }
}
```

This Apex policy example implements a policy that is triggered when a session is created from a specific IP address.

Example:

```
global class SessionPolicyCondition implements TxnSecurity.PolicyCondition {
  public boolean evaluate(TxnSecurity.Event e) {
    AuthSession eObj = [SELECT SourceIp FROM AuthSession WHERE Id = :e.entityId];
    if(eObj.SourceIp == '1.1.1.1' ){
      return true;
    }
    return false;
  }
}
```

This DataExport policy implements a policy that is triggered when someone exports data via the Data Loader.

Example:

```
global class DataExportPolicyCondition implements TxnSecurity.PolicyCondition {
  public boolean evaluate(TxnSecurity.Event e) {
    if(e.data.get('SourceIp') == '1.1.1.1' ){
      return true;
    }
    return false;
  }
}
```

This Apex policy is triggered when someone accesses reports.

Example:

```
global class ReportsPolicyCondition implements TxnSecurity.PolicyCondition {
  public boolean evaluate(TxnSecurity.Event e) {
    if(e.data.get('SessionLevel') == 'STANDARD' ){
      return true;
    }
    return false;
  }
}
```

This Apex policy is triggered when someone accesses a Connected App.

Example:

```
global class ConnectedAppsPolicyCondition implements TxnSecurity.PolicyCondition {
  public boolean evaluate(TxnSecurity.Event e) {
   if(e.data.get('SessionLevel') == 'STANDARD' && (e.entityId == '0CiD00000004Cce')){

      return true;
    }
    return false;
  }
}
```

SEE ALSO:

Additional PolicyCondition Example Implementations

Apex DML Operations

Manage Transaction Security Policies

Use Transaction Security policies to define, enable, and generate Apex code to implement your policies. Specify how to be notified when a policy is triggered, and then select the policies to enable. Only an active user assigned the System Administrator profile can use this feature.

1. From Setup, enter `Transaction Security` in the `Quick Find` box, then select **Transaction Security**.
2. From the Transaction Security Policies page, you can
   - Edit a view
   - Create a view
   - Edit a policy
   - Create a policy
   - Edit the `TxnSecurity.PolicyCondition` Apex class for a policy
   - Delete a policy
   - Set the transaction security default preferences

You can change the transaction security default preferences at any time.

EDITIONS

Available in: Lightning Experience

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

Requires purchasing Salesforce Shield or Salesforce Shield Event Monitoring add-on subscriptions.

USER PERMISSIONS

User Permissions Needed
To create, edit, and manage transaction security policies: • Customize Application
To manage transaction security policies: • Author Apex

Receiving Transaction Security Notifications

You receive the notifications you've selected when an enabled policy is triggered. The notifications are formatted for easy recognition.

EDITIONS

Available in: Lightning Experience

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

Requires purchasing Salesforce Shield or Salesforce Shield Event Monitoring add-on subscriptions.

Email Notifications

Email notifications are sent from Transaction Security with subject "Transaction Security Alert!" The body of the message contains the policy that was triggered and the event or events that occurred to trigger the policy. The times listed are when the policy was triggered in the recipient's locale and time zone. For example, a policy is triggered at 6:46 PM in the Eastern Standard Time zone. The administrator receiving the notification is in the Pacific Standard Time zone, so the times are shown as PST. Here's an example.

Example:

```
From: Transaction Security <noreply@salesforce.com>
To: Admin@company.com
Sent: Friday, November 12, 2014, 5:35 PM
Subject: Transaction Security Alert!

This is a transaction security policy alert.
```

```
Policy: An administrator created a new user.

Event(s) responsible for triggering this policy:
1. Created new user Lisa Johnson at 11/12/2014 5:35:09 PM PST
```

In-App Notifications

In-app notifications are available only if you're a Salesforce for Android or Salesforce for iOS user. The notification lists the policy that was triggered. Here's an example.

Example:

```
Transaction Security Alert:
Policy New Encrypted Custom Field was triggered.
```

Single Sign-On

Single sign-on (SSO) lets users access authorized network resources with one login. You validate usernames and passwords against your corporate user database or other client app rather than Salesforce managing separate passwords for each resource.

Salesforce offers the following ways to use SSO.

- Federated authentication using Security Assertion Markup Language (SAML) lets you send authentication and authorization data between affiliated but unrelated web services. You can log in to Salesforce from a client app. Salesforce enables federated authentication for your org automatically.
- Delegated authentication SSO integrates Salesforce with an authentication method that you choose. You can integrate authentication with your LDAP (Lightweight Directory Access Protocol) server or use a token instead of a password for authentication. You manage delegated authentication at the permission level, not at the org level, giving you more flexibility. With permissions, you can require some to use delegated authentication while others use their Salesforce-managed password.

  Delegated authentication offers the following benefits.

  - Uses a stronger form of user authentication, such as integration with a secure identity provider
  - Makes your login page private and accessible only behind a corporate firewall
  - Differentiates your org from all other companies that use Salesforce to reduce phishing attacks

  You must contact Salesforce to enable delegated authentication before you can configure it on your org.
- Authentication providers let your users log in to your Salesforce org using their login credentials from an external service provider. Salesforce supports the OpenID Connect protocol, which lets users log in from any OpenID Connect provider, such as Google, PayPal, and LinkedIn. When an authentication provider is enabled, Salesforce doesn't validate a user's password. Instead, Salesforce uses the user's login credentials from the external service provider to establish authentication credentials.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Federated Authentication is available in: **All** Editions

Delegated Authentication is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Authentication Providers are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view the settings:
- View Setup and Configuration

To edit the settings:
- Customize Application

  AND

  Modify All Data

When you have an external identity provider and configure SSO for your Salesforce org, Salesforce is then acting as a service provider. You can also enable Salesforce as an identity provider and use SSO to connect to a different service provider. Only the service provider needs to configure SSO.

The Single Sign-On Settings page displays which version of SSO is available for your org. To learn more about SSO settings, see Configure SAML Settings for Single Sign-On. For more information about SAML and Salesforce security, see the *Security Implementation Guide*.

Benefits of SSO

Implementing SSO brings several advantages to your org.

- **Reduced administrative costs**—With SSO, users memorize a single password to access network resources and external apps and Salesforce. When accessing Salesforce from inside the corporate network, users log in seamlessly and aren't prompted for a username or password. When accessing Salesforce from outside the corporate network, the users' corporate network login works to log them in. With fewer passwords to manage, system admins receive fewer requests to reset forgotten passwords.
- **Leverage existing investment**—Many companies use a central LDAP database to manage user identities. You can delegate Salesforce authentication to this system. Then when users are removed from the LDAP system, they can no longer access Salesforce. Users who leave the company automatically lose access to company data after their departure.
- **Time savings**—On average, users take 5–20 seconds to log in to an online app. It can take longer if they mistype their username or password and are prompted to reenter them. With SSO in place, manually logging in to Salesforce is avoided. These saved seconds reduce frustration and add up to increased productivity.
- **Increased user adoption**—Due to the convenience of not having to log in, users are more likely to use Salesforce regularly. For example, users can send email messages that contain links to information in Salesforce, such as records and reports. When the recipient of the email message clicks the links, the corresponding Salesforce page opens.
- **Increased security**—All password policies that you've established for your corporate network are in effect for Salesforce. Sending an authentication credential that's only valid for a single time also increases security for users who have access to sensitive data.

IN THIS SECTION:

Best Practices for Implementing Single Sign-On

Salesforce offers a set of best practices that you can follow when implementing delegated authentication, federated authentication using SAML, single sign-on (SSO) for portals, and SSO for Sites.

Delegated Authentication Single Sign-On

You can integrate Salesforce with the authentication method of your choice using delegated authentication single sign-on (SSO). You can integrate with your LDAP (Lightweight Directory Access Protocol) server or authenticate with a token instead of a password. You manage delegated authentication at the permission level, not at the org level, giving you more flexibility. With permissions, you can require some to use delegated authentication while others use their Salesforce-managed password.

Configure Salesforce for Delegated Authentication

You manage delegated authentication at the permission level, not at the org level, giving you more flexibility. With permissions, you can require some to use delegated authentication while others use their Salesforce-managed password. You must contact Salesforce to enable the delegated authentication feature before you can configure it in your org.

Control Individual API Client Access to Your Salesforce Org

You can restrict access to API client apps, such as Data Loader, the Salesforce app, and third-party apps. To restrict access, request the API client whitelisting feature from Salesforce. When whitelisting is enabled, you restrict access to all connected apps until you explicitly approve each app. Approved apps are often called whitelisted apps.

Viewing Single Sign-On Login Errors

SAML

Salesforce Identity uses the XML-based Security Assertion Markup Language (SAML) protocol for single sign-on into Salesforce from a corporate portal or identity provider. With SAML, you can transfer user information between services, such as from Salesforce to Microsoft 365.

About Just-in-Time Provisioning for SAML

External Authentication Providers

Authentication providers let your users log in to your Salesforce org using their login credentials from an external service provider. Salesforce provides authentication providers for apps that support the OpenID Connect protocol, such as Google, Facebook, Twitter, and LinkedIn. For apps that don't support OpenID Connect, Salesforce provides an Apex `Auth.AuthProviderPluginClass` abstract class to create a custom authentication provider.

Using Frontdoor.jsp to Log Into Salesforce

You can use frontdoor.jsp to give users access to Salesforce from a custom Web interface, such as a remote access Force.com site, using their existing session ID and the server URL.

Use Request Parameters with Client Configuration URLs

Add functionality to your authentication provider with request parameters. For example, you can use these parameters to direct users to log in to specific sites, get customized permissions from the third party, or go to a specific location after authenticating.

Identity Providers and Service Providers

An *identity provider* is a trusted provider that lets you use single sign-on (SSO) to access other websites. A *service provider* is a website that hosts apps. You can enable Salesforce as an identity provider and define one or more service providers. Your users can then access other apps directly from Salesforce using SSO. SSO can be a great help to your users—instead of having to remember many passwords, they only have to remember one.

Configure Remote Site Settings

Named Credentials

A named credential specifies the URL of a callout endpoint and its required authentication parameters in one definition. To simplify the setup of authenticated callouts, specify a named credential as the callout endpoint. If you instead specify a URL as the callout endpoint, you must register that URL in your org's remote site settings and handle the authentication yourself. For example, for an Apex callout, your code would need to handle authentication, which can be less secure and especially complicated for OAuth implementations.

Identity Connect

Identity Connect integrates Microsoft Active Directory (AD) with Salesforce. User information entered in AD is shared with Salesforce seamlessly and instantaneously. Companies that use AD for user management can use Identity Connect to manage Salesforce accounts.

Single Logout

With single logout (SLO), your users log out from one application, and are automatically logged out from other applications they are using.

Best Practices for Implementing Single Sign-On

Salesforce offers a set of best practices that you can follow when implementing delegated authentication, federated authentication using SAML, single sign-on (SSO) for portals, and SSO for Sites.

Salesforce offers the following ways to use SSO.

- Federated authentication using Security Assertion Markup Language (SAML) lets you send authentication and authorization data between affiliated but unrelated web services. You can log in to Salesforce from a client app. Salesforce enables federated authentication for your org automatically.
- Delegated authentication SSO integrates Salesforce with an authentication method that you choose. You can integrate authentication with your LDAP (Lightweight Directory Access Protocol) server or use a token instead of a password for authentication. You manage delegated authentication at the permission level, not at the org level, giving you more flexibility. With permissions, you can require some to use delegated authentication while others use their Salesforce-managed password.

  Delegated authentication offers the following benefits.

  - Uses a stronger form of user authentication, such as integration with a secure identity provider
  - Makes your login page private and accessible only behind a corporate firewall
  - Differentiates your org from all other companies that use Salesforce to reduce phishing attacks

  You must contact Salesforce to enable delegated authentication before you can configure it on your org.
- Authentication providers let your users log in to your Salesforce org using their login credentials from an external service provider. Salesforce supports the OpenID Connect protocol, which lets users log in from any OpenID Connect provider, such as Google, PayPal, and LinkedIn. When an authentication provider is enabled, Salesforce doesn't validate a user's password. Instead, Salesforce uses the user's login credentials from the external service provider to establish authentication credentials.

In addition, you can also configure SAML for use with portals as well as for Sites.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Federated Authentication is available in: **All** Editions

Delegated Authentication is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Customer Portals and partner portals are not available in **Database.com**

USER PERMISSIONS

To view the settings:
- View Setup and Configuration

To edit the settings:
- Customize Application

  AND

  Modify All Data

Delegated Authentication Best Practices

Consider these best practices when implementing delegated authentication SSO for your org.

- Your org's implementation of the web service must be accessible by Salesforce servers, so you must deploy the web service on a server in your DMZ. Remember to use your server's external DNS name when entering the delegated gateway URL in the Delegated authentication section in Salesforce. From Setup, enter `Single Sign-On Settings` in the `Quick Find` box, then select **Single Sign-On Settings**.
- If Salesforce and your system can't connect, or if the request takes longer than 10 seconds to process, the login attempt fails. The user gets an error message indicating that the corporate authentication service is down.
- Namespaces, element names, and capitalization must be exact in SOAP requests. Wherever possible, generate your server stub from the WSDL file to ensure accuracy.
- For security reasons, make your web service available by TLS. A certificate from a trusted provider, such as Verisign or Thawte, is required. For a list of trusted providers, contact Salesforce.

- The IP address that originated the login request is sourceIp. Use this information to restrict access based on the user's location. Also, the Salesforce feature that validates login IP ranges applies to SSO users. For more information, see Restrict Where and When Users Can Log In to Salesforce on page 574.
- You might need to map your org's internal usernames to your Salesforce usernames. If your org doesn't follow a standard mapping, try extending your user database schema (for example, Active Directory) to include the Salesforce username as an attribute of a user account. Your authentication service can then use this attribute to map back to a user account.
- We recommend that you don't enable SSO for Salesforce admins. If your Salesforce admins are SSO users and your SSO server has an outage, they have no way to log in to Salesforce. Make sure that Salesforceadmins can log in to Salesforce so that they can disable SSO if problems occur.
- We recommend that you use a Developer Edition account or a sandbox when developing a SSO solution before implementing it in your org. To sign up for a free Developer Edition account, go to developer.salesforce.com.
- Make sure to test your implementation with Salesforce clients, such as Salesforce for Outlook, Connect for Office, and Connect Offline. For more information, see Single Sign-On for Salesforce clients.

Federated Authentication Using SAML Best Practices

Consider these best practices when implementing federated SSO with SAML for your org.

- Get the Salesforce login URL from the Single Sign On Settings configuration page and enter it in the corresponding configuration parameter of your identity provider. Sometimes, the setting is called the recipient URL.
- Salesforce allows a maximum of 3 minutes for clock skew with your IDP server. Make sure that your server's clock is up to date.
- If you can't log in with SAML assertion, check the login history and note the error message. Use the SAML Assertion Validator on the Single Sign On Settings configuration page to troubleshoot.
- Map your orgs internal usernames and Salesforce usernames. To map the names, you can add a unique identifier to the `FederationIdentifier` field of each Salesforce user. Or you can extend your user database schema (for example, Active Directory) to include the Salesforce username as an attribute of a user account. Choose the corresponding option for the `SAML Identity Type` field, and configure your authentication service to send the identifier in SAML assertions.
- Before allowing users to log in with SAML assertions, enable the SAML org preference and provide the necessary configurations.
- Use the My Domain feature to prevent users from logging in to Salesforce directly, and give admins more control over login policies. You can use the URL parameters provided in the `Salesforce Login URL` value from the Single Sign-On Settings configuration page with your custom domain.

  For example, if the `Salesforce Login URL` is `https://login.salesforce.com/?saml=02HKiP...`

  you can use `https://`*`yourDomain`*`.my.salesforce.com/?saml=02HKiP...`
- We recommend that you use a Developer Edition account or a sandbox when testing a SAML SSO solution. To sign up for a free Developer Edition account, go to developer.salesforce.com.
- Sandbox copies are made with federated authentication with SAML disabled. Any configuration information is preserved, except the value for `Salesforce Login URL`. The `Salesforce Login URL` is updated to match your sandbox URL, for example `https://`*`yourInstance`*`.salesforce.com/`, after you re-enable SAML. To enable SAML in the sandbox, from Setup, enter *`Single Sign-On Settings`* in the `Quick Find` box, then select **Single Sign-On Settings**; then click **Edit**, and select `SAML Enabled`.
- Your identity provider must allow you to set the service provider's audience URL. The value must match the `Entity ID` value in the SSO configuration. The default is `https://saml.salesforce.com`.

SSO for Portals Best Practices

Customer Portals and partner portals are not available for new orgs as of the Summer '13 release. Use Communities instead. For more information about SSO and SAML for Communities, see "Configuring SAML for Communities" in the Salesforce Help. If you continue to use portals, be aware of these requirements.

- Only SAML version 2.0 can be used with portals.
- Only Customer Portals and partner portals are supported.
- Service provider initiated login is not supported.
- Both the `portal_id` and `organization_id` attributes are required. If only one is specified, the user receives an error.
- If both the `portal_id` and `organization_id` attributes are populated in the SAML assertion, the user is directed to that portal login. If neither is populated, the user is directed to the regular SAML Salesforce login.
- More than one portal can be used with a single org.

SSO for Sites Best Practices

- Only SAML version 2.0 can be used with Sites.
- Only Customer Portals and partner portals are supported.
- Service provider initiated login is not supported.
- The `portal_id`, `organization_id`, and `siteUrl` attributes are required. If only one is specified, the user receives an error.
- If all the `portal_id`, `organization_id` and `siteUrl` attributes are populated in the SAML assertion, the user is directed to that Sites login. If the `siteUrl` isn't populated and the other two are, the user is directed to the portal login.
- More than one portal can be used with a single org.

SEE ALSO:

Single Sign-On

Single Sign-On Implementation Guide

Delegated Authentication Single Sign-On

You can integrate Salesforce with the authentication method of your choice using delegated authentication single sign-on (SSO). You can integrate with your LDAP (Lightweight Directory Access Protocol) server or authenticate with a token instead of a password. You manage delegated authentication at the permission level, not at the org level, giving you more flexibility. With permissions, you can require some to use delegated authentication while others use their Salesforce-managed password.

Here's the process that Salesforce uses to authenticate users with delegated authentication SSO.

1. When a user tries to log in—either online or using the API—Salesforce validates the username and checks the user's permissions and access settings.
2. If the user has the "Is Single Sign-On Enabled" user permission, Salesforce doesn't validate the username and password. Instead, a web services call is made to the user's org asking it to validate the username and password.

   Note: Salesforce doesn't store, log, or view the password. It's disposed of immediately after the process completes.

3. The web services call passes the username, password, and sourceIp to your web service. Source Ip is the IP address where the login request originated. You must create and deploy an implementation of the web service that Salesforce servers can access.
4. Your web service implementation validates the passed information and returns either `true` or `false`.
5. If the response is `true`, the login process continues, a new session is generated, and the user proceeds to the app. If `false`, the user gets an error message that the username and password combination is invalid.

Note: With delegated authentication, a user can experience a slight delay when logging in while the user account becomes available in the org.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Modify All Data

SEE ALSO:

Single Sign-On

Administrator setup guide: Single Sign-On Implementation Guide

Configure Salesforce for Delegated Authentication

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Modify All Data

You manage delegated authentication at the permission level, not at the org level, giving you more flexibility. With permissions, you can require some to use delegated authentication while others use their Salesforce-managed password. You must contact Salesforce to enable the delegated authentication feature before you can configure it in your org.

1. Build your SSO web service.

   a. In Salesforce, download the Web Services Description Language (WSDL) file `AuthenticationService.wsdl`. From Setup, enter *`API`* in the `Quick Find` box, then select **API**, then select **Download Delegated Authentication WSDL**.

      The WSDL file describes the delegated authentication SSO service. Use the WSDL file to generate a server-side stub to which you add your SSO implementation. For example, in the WSDL2Java tool from Apache Axis, use the `--server-side` switch. With the .NET wsdl.exe tool, use the `/server` switch.

      For a sample request and response, see Sample SOAP Message for Delegated Authentication on page 652.

   b. Add a link to your corporate intranet or other internal site that takes the authenticated user's credentials and passes them through an HTTP POST to the Salesforce login page.

      Because Salesforce doesn't use the password field other than to pass it back to you, don't pass in a password. Instead, pass another authentication token, such as a Kerberos Ticket, so that your corporate passwords aren't passed to or from Salesforce.

      You can configure the Salesforce delegated authentication authority to accept only a token or either a tokenor password. If the authority accepts only a token, Salesforce users can't log in to Salesforce directly because they can't create a valid token. However, many authorities support both tokens and passwords In this case, users can log in to Salesforce through the login page.

      When the Salesforce server passes the credentials back to you in the `Authenticate` message, verify them. Then the user can access the app.

2. In Salesforce, specify your org's SSO gateway URL. From Setup, enter *`Single Sign-On`* in the `Quick Find` box, select **Single Sign-On Settings**, and then click **Edit**. Enter the URL in the Delegated Gateway URL text box. For security reasons, Salesforce restricts outbound ports to one of the following.

   - 80, which accepts only HTTP connections
   - 443, which accepts only HTTPS connections
   - 1024–66535, which accept HTTP or HTTPS connections

3. Optionally, select **Force Delegated Authentication Callout**.

   Note: Select this option if you must record every login attempt. This option forces a callout to the SSO endpoint regardless of login restriction failures. If you don't select this option, a call isn't made to the SSO endpoint if the first login attempt fails due to login restrictions within the Salesforce org.

4. Enable the "Is Single Sign-On Enabled" permission.

Important: If single sign-on (SSO) is enabled for your org, API and desktop client users can log in to Salesforce unless their profile has IP address restrictions set and they try to log in from outside of the range defined. Also the SSO authority usually handles login lockout policies for users with the "Is Single Sign-On Enabled" permission. However, if the security token is enabled for your org, your org's login lockout settings determine how many times users can attempt to log in with an invalid security token before being locked out of Salesforce.

SEE ALSO:

- Single Sign-On
- Delegated Authentication Single Sign-On

Control Individual API Client Access to Your Salesforce Org

You can restrict access to API client apps, such as Data Loader, the Salesforce app, and third-party apps. To restrict access, request the API client whitelisting feature from Salesforce. When whitelisting is enabled, you restrict access to all connected apps until you explicitly approve each app. Approved apps are often called whitelisted apps.

Client apps are external apps that access your org through the API. Salesforce requires you to create a connected app for each client app to provide authentication capabilities. Authentication ensures that users access Salesforce data without revealing username and password credentials. All client applications that aren't configured as connected apps are denied access to your Salesforce org.

Note: Contact Salesforce to get the API client whitelisting feature. After it's enabled, all client access to a connected app is restricted until the Salesforce admin explicitly allows (whitelists) it. This restriction can block access to some apps that your users are using. To avoid unintentional blocks, you can give the users the Use Any API Client permission. Be careful when using this permission. As the name implies, you're giving up a lot of control.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Modify All Data

Step 1: Set Up App Access in Your Org

1. Contact Salesforce to get the API client whitelisting feature enabled for your org.
2. From Setup, enter `Connected Apps` in the Quick Find box, then select **Connected Apps**.
3. Under the App Access Settings, click **Edit**.
4. Select the option, **Limit API access to connected apps to those with the policy, Admin approved users are pre-authorized.**
5. Select **Allow Visualforce pages to bypass this restriction** so that Visualforce pages behave as expected. If unselected, client applications that call `getSessionId()` are denied access. Also, apps that make API calls to Salesforce using a session obtained in a Visualforce context are denied access.
6. Click **Save**.

Step 2: Restrict OAuth Connected App Access (Whitelist Apps)

1. From Setup, enter `Connected Apps` in the Quick Find box and select **Connected Apps**.
2. Select the name of the connected app.
3. Click **Edit Policies**, then Under OAuth policies, select **Admin approved users are pre-authorized**.
4. Click **Save**.

Step 3: Grant Users Access to OAuth Connected Apps

You give users access to connected apps through permissions. Typically, a list of available connected apps appears under permissions. Then you select which apps to authorize. If a connected app doesn't appear on the list, no one has tried to access the org with it yet.

Determine Whether an OAuth Connected App Is Whitelisted

1. From Setup, enter `Connected Apps` in the Quick Find box and select **Connected Apps OAuth Usage**.

2. Under Actions, if **Unblock** is disabled, the connected app was blocked because API Client Whitelisting is enabled for the org and the connected app isn't whitelisted.
3. To whitelist the connected app, install the app, and set the app's OAuth policy Permitted Users option to **Admin approved users are pre-authorized**.
4. Grant users access to the connected app.

Note: Salesforce creates connected apps for common Salesforce apps, and installs them in your org automatically. It's your responsibility to whitelist the connected apps and assign which users can access them.

If users have the Use Any API Client permission, they can access any app, including connected apps having the OAuth policy, Admin approved users are pre-authorized. The User Any API Client permission is intended for a limited number of admins.

Viewing Single Sign-On Login Errors

If your organization is enabled for Single Sign-On using delegated authentication and has built a Single Sign-On solution, you can view the most recent Single Sign-On login errors for your organization.

1. From Setup, enter `Delegated Authentication Error History` in the `Quick Find` box, then select **Delegated Authentication Error History**.
2. For the twenty-one most recent login errors, you can view the user's username, login time, and the error.

USER PERMISSIONS

To view Single Sign-On login errors:

- Modify All Data

Note: Contact Salesforce to learn more about enabling Single Sign-On for your organization.

SEE ALSO:

Single Sign-On

SAML

Salesforce Identity uses the XML-based Security Assertion Markup Language (SAML) protocol for single sign-on into Salesforce from a corporate portal or identity provider. With SAML, you can transfer user information between services, such as from Salesforce to Microsoft 365.

The identity provider performs most of the work to set up single sign-on (SSO).

1. Establish a SAML identity provider and gather information about how they connect to Salesforce. The identity provider sends SSO requests to Salesforce.
2. Provide information to your identity provider, such as the URLs for the start and logout pages.
3. Configure Salesforce using the instructions in Configure SAML Settings for Single Sign-On. Only this step takes place in Salesforce.

Your identity provider sends SAML assertions to Salesforce using the SAML Web Single Sign-on Browser POST profile. Salesforce sends SAML responses to the identity provider login URL specified under Setup by entering *`Single Sign-On`* in the `Quick Find` box, then selecting **Single Sign-On Settings**. Salesforce receives the assertion, verifies it against your Salesforce configuration, and, if the assertion is true, allows SSO.

If you have problems with the SAML assertion after you configure Salesforce for SAML, use the SAML Assertion Validator to validate the SAML assertion. You can obtain a SAML assertion from your identity provider.

If your users can't log in using SAML, review the SAML login history to determine why. Sharing the login history with your identity provider helps resolve problems quickly.

Click **Download Metadata** to download an XML file of your SAML configuration settings to send to your identity provider. The identity provider can then upload these configuration settings to connect to your Salesforce orgcommunity.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Federated Authentication is available in: **All** Editions

Delegated Authentication is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Authentication Providers are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view the settings:
- View Setup and Configuration

To edit the settings:
- Customize Application

  AND

  Modify All Data

IN THIS SECTION:

Working With Your Identity Provider

1. You must gather the following information from your identity provider before configuring Salesforce for SAML.
   - The version of SAML the identity provider uses (1.1 or 2.0)
   - The entity ID of the identity provider (also known as the issuer)
   - An authentication certificate.

     Tip: Be sure to store the certificate where you can access it from your browser. This will be uploaded to Salesforce in a later step.
   - The following SAML assertion parameters, as appropriate:
     - The SAML user ID type
     - The SAML user ID location
     - Attribute Name
     - Attribute URI
     - Name ID format

     Note: Attribute Name, Attribute URI, and Name ID format are only necessary if the `SAML User ID Location` is in an Attribute element, and not the name identifier element of a Subject statement.

     Tip: To set up single sign-on quickly, you can import SAML 2.0 settings from an XML file (or a URL pointing to the file) on the Single Sign-On Settings page. Obtain the XML from your identity provider.

   You may also want to share more information about these values with your identity provider.

   Tip: Enable Salesforce for SAML and take a screenshot of the page for your identity provider. From Setup, enter *`Single Sign-On Settings`* in the `Quick Find` box, then select **Single Sign-On Settings**, click **Edit**, then select `SAML Enabled`.

2. Work with your identity provider to setup the start, login, and logout pages.
3. Share the example SAML assertions with your identity provider so they can determine the format Salesforce requires for successful single sign-on.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Federated Authentication is available in: **All** Editions

Delegated Authentication is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Authentication Providers are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view the settings:
- View Setup and Configuration

To edit the settings:
- Customize Application

  AND

  Modify All Data

SEE ALSO:

SAML

Configure SAML Settings for Single Sign-On

From this page, you can configure your org to use single sign-on. You can also set up just-in-time provisioning. Work with your identity provider to properly configure these settings. For more information about single sign-on, see Single Sign-On. For more information about just-in-time provisioning, see About Just-In-Time Provisioning.

To configure SAML settings for single sign-on from your corporate identity provider to Salesforce:

1. Gather information from your identity provider.
2. Provide information to your identity provider.
3. Set up single sign-on.
4. Set up an identity provider to encrypt SAML assertions (optional).
5. Enable Just-in-Time user provisioning (optional).
6. Edit the SAML JIT handler if you selected `Custom SAML JIT with Apex Handler` for Just-in-Time provisioning.
7. Test the single sign-on connection.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Federated Authentication is available in: **All** Editions

Delegated Authentication is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Authentication Providers are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view the settings:
- View Setup and Configuration

To edit the settings:
- Customize Application

  AND

  Modify All Data

Set up single sign-on

1. In Salesforce, from Setup, enter *`Single Sign-On Settings`* in the `Quick Find` box, then select **Single Sign-On Settings**, and click **Edit**.
2. Select `SAML Enabled`. You must enable SAML to view the SAML single sign-on settings.
3. Specify the SAML version used by your identity provider.
4. Click **Save**.
5. In SAML Single Sign-On Settings, click the appropriate button to create a configuration, as follows.
   - **New** - Specify all settings manually.
   - **New from Metadata File** - Import SAML 2.0 settings from an XML file from your identity provider. This option reads the XML file and uses it to complete as many of the settings as possible.

     Note: If your XML file contains information for more than one configuration, the first configuration that occurs in the XML file is used.
   - **New from Metadata URL** - Import SAML 2.0 settings from a public URL. This option reads the XML file at a public URL and uses it to complete as many of the settings as possible. The URL must be added to Remote Site Settings to access it from your Salesforce org.
6. Give this setting a **Name** for reference within your org.

   Salesforce inserts the corresponding **API Name** value, which you can customize if necessary.
7. Enter the `Issuer`. Often referred to as the entity ID for the identity provider.
8. If your Salesforce org has domains deployed, specify whether you want to use the base domain (`https://saml.salesforce.com`) or the custom domain for the **Entity ID**. You must share this information with your identity provider.

Tip: Generally, use the custom domain as the entity ID. If you already have single sign-on configured before deploying a domain, the base domain is the entity ID. If you are providing Salesforce to Salesforce services, you must specify the custom domain.

9. For the `Identity Provider Certificate`, use the **Browse** button to locate and upload the authentication certificate issued by your identity provider.
10. For the `Request Signing Certificate`, select the certificate you want from the ones saved in your **Certificate and Key Management** settings.
11. For the `Request Signature Method`, select the hashing algorithm for encrypted requests, either `RSA-SHA1` or `RSA-SHA256`.
12. Optionally, if the identity provider encrypts SAML assertions, select the `Assertion Decryption Certificate` they're using from the ones saved in your **Certificate and Key Management** settings. This field is available only if your org supports multiple single sign-on configurations. For more information, see Set up an identity provider to encrypt SAML assertions.
13. For the `SAML Identity Type`, `SAML Identity Location`, and other fields described in Identity Provider Values, specify the values provided by your identity provider as appropriate.
14. For the `Service Provider Initiated Request Binding`, select the appropriate value based on the information provided by your identity provider.
15. For SAML 2.0, if your identity provider has specific login or logout pages, specify them in **Identity Provider Login URL** and **Identity Provider Logout URL**, respectively.

    Note: These fields appear in Developer Edition and sandbox organizations by default and in production organizations only if My Domain is enabled. The fields do not appear in trial organizations or sandboxes linked to trial organizations.

16. For the `Custom Error URL`, specify the URL of the page that the users are directed to if there's an error during SAML login. It must be a publicly accessible page, such as a public site Visualforce page. The URL can be absolute or relative.
17. Optionally, set up Just-in-Time user provisioning. For more information, see Enable Just-in-Time user provisioning and About Just-in-Time Provisioning for SAML.
18. Click **Save**.

Click **Download Metadata** to download an XML file of your SAML configuration settings to send to your identity provider. The identity provider can then upload these configuration settings to connect to your Salesforce orgcommunity.

Set up an identity provider to encrypt SAML assertions

When Salesforce is the service provider for inbound SAML assertions, you can pick a saved certificate to decrypt inbound assertions from third party identity providers. You need to provide a copy of this certificate to the identity provider.

1. In the Single Sign-On Settings page in Setup, add a new SAML configuration.
2. In the `Assertion Decryption Certificate` field, specify the certificate for encryption from the ones saved in your **Certificate and Key Management** settings.

    Note: If you don't see the `Assertion Decryption Certificate` field you need to enable multiple single sign-on for your organization.(Applies to orgs created before the Summer '13 release that aren't using SAML 1.1).To enable multiple single sign-on configurations, select **Enable Multiple Configs** on the **Single Sign-On Settings** page. If this setting has already been enabled, the field appears, and you won't see the **Enable Multiple Configs** button.

3. Set the `SAML Identity Location` to the element where your identifier is located.

4. When you save the new SAML configuration, your org's SAML settings value for the `Salesforce Login URL` (also known as the "Salesforce ACS URL") changes. Get the new value (from the Single Sign-On Settings page in Setup), and click the name of the new SAML configuration. The value is in the `Salesforce Login URL` field.
5. The identity provider must use the `Salesforce Login URL` value.
6. You also need to provide the identity provider with a copy of the certificate selected in the `Assertion Decryption Certificate` field to use for encrypting assertions.

Enable Just-in-Time user provisioning

1. In SAML Single Sign-On Settings, select `User Provisioning Enabled`.
   - `Standard` - This option allows you to provision users automatically using attributes in the assertion.
   - `Custom SAML JIT with Apex handler` - This option provisions users based on logic in an Apex class.
2. If you selected `Standard`, click **Save** and test the single sign-on connection.. If you selected `Custom SAML JIT with Apex handler`, proceed to the next step.
3. In the `SAML JIT Handler` field, select an existing Apex class as the SAML JIT handler class. This class must implement the SamlJitHandler interface. If you do not have an Apex class, you can generate one by clicking `Automatically create a SAML JIT handler template`. You must edit this class and modify the default content before using it. For more information, see Edit the SAML JIT handler.
4. In the `Execute Handler As` field, select the user that runs the Apex class. The user must have "Manage Users" permission.
5. Just-in-time provisioning requires a Federation ID in the user type. In `SAML Identity Type`, select `Assertion contains the Federation ID from the User object`. If your identity provider previously used the Salesforce username, communicate to them that they must use the Federation ID.
6. Click **Save**.

Edit the SAML JIT handler

1. From Setup, enter *`Apex Classes`* in the `Quick Find` box, then select **Apex Classes**.
2. Edit the generated Apex SAML JIT handler to map fields between SAML and Salesforce. In addition, you can modify the generated code to support the following:
   - Custom fields
   - Fuzzy profile matching
   - Fuzzy role matching
   - Contact lookup by email
   - Account lookup by account number
   - Standard user provisioning into a community
   - Standard user login into a community
   - Default profile ID usage for portal Just-in-Time provisioning
   - Default portal role usage for portal Just-in-Time provisioning
   - Username generation for portal Just-in-Time provisioning

   For example, to support custom fields in the generated handler code, find the "Handle custom fields here" comment in the generated code. After that code comment, insert your custom field code. For more information and examples, see the SamlJitHandler Interface documentation.

Note: If your identity provider sends JIT attributes for the Contact or Account object with the User object in the same assertion, the generated handler might not be able to make updates. For a list of User fields that cannot be updated at the same time as the Contact or Account fields, see sObjects That Cannot Be Used Together in DML Operations.

Test the single sign-on connection

After you have configured and saved your SAML settings, test them by trying to access the identity provider's application. Your identity provider directs the user's browser to POST a form containing SAML assertions to the Salesforce login page. Each assertion is verified, and if successful, single sign-on is allowed.

If you have difficulty signing on using single sign-on after you have configured and saved your SAML settings, use the SAML Assertion Validator. You might have to obtain a SAML assertion from your identity provider first.

If your users are having problems using SAML to log in, you can review the SAML login history to determine why they were not able to log in and share that information with your identity provider.

If you are using SAML version 2.0, after you've finished configuring SAML, the OAuth 2.0 Token Endpoint field is populated. Use the tokenwith the web single sign-on authentication flow for OAuth 2.0.

SEE ALSO:

SAML

Best Practices for Implementing Single Sign-On

Validating SAML Settings for Single Sign-On

Administrator setup guide: Single Sign-On Implementation Guide

Certificates and Keys

View and Edit Single Sign-On Settings

After you've configured your Salesforce org to use SAML, you can manage the SAML configuration from the Single Sign-On Settings page.

From Setup, enter *`Single Sign-On Settings`* in the `Quick Find` box, then select **Single Sign-On Settings**.

After the SAML configuration completes, the Single Sign-On Settings page displays the generated URLs and OAuth 2.0 token endpoint.

Field	Description
`Salesforce Login URL`	For SAML 2.0. The URL associated with the login for the Web SSO OAuth assertion flow. This URL appears if you configured SAML with "Assertion contains the User's Salesforce username" for `SAML Identity Type` and "Identity is in the NameIdentifier element of the Subject statement" for `SAML Identity Location`.
`Salesforce Logout URL`	For SAML 2.0. The Salesforce logout URL that users are directed to after they log off. This URL appears if you didn't specify a value for `Identity Provider Logout URL`.
`OAuth 2.0 Token Endpoint`	For SAML 2.0. The ACS URL used when enabling Salesforce as an identity provider in the Web SSO OAuth assertion flow.

From this page you can do any of the following:

- Click **Edit** to change the existing SAML configuration.
- Click **SAML Assertion Validator** to validate the SAML settings for your org using a SAML assertion provided by your identity provider.
- Click **Download Metadata** to download an XML file of your SAML configuration settings to send to your identity provider. The identity provider can then upload these configuration settings to connect to your Salesforce orgcommunity. Enabled only if your identity provider supports metadata and if you are using SAML 2.0.

SEE ALSO:

SAML

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Federated Authentication is available in: **All** Editions

Delegated Authentication is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Authentication Providers are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Modify All Data

Identity Provider Values

Before you can configure Salesforce for SAML, you must receive information from your identity provider. This information must be used on the single sign-on page.

The following information might be useful for your identity provider.

Field	Description
`SAML Version`	The version of SAML your identity provider uses. Salesforce currently supports version 1.1 and 2.0. The SAML specifications for the various versions are linked below: • SAML 1.1 • SAML 2.0
`Issuer`	The Entity ID—a URL that uniquely identifies your SAML identity provider. SAML assertions sent to Salesforce must match this value exactly in the `<saml:Issuer>` attribute of SAML assertions.
`Entity ID`	The issuer in SAML requests generated by Salesforce, and is also the expected audience of any inbound SAML Responses. If you don't have domains deployed, this value is always `https://saml.salesforce.com`. If you have domains deployed, Salesforce recommends that you use your custom domain name. You can find the value on the Single Sign-On Settings page. From Setup, enter *`Single Sign-On Settings`* in the `Quick Find` box, then select **Single Sign-On Settings**.
`Identity Provider Certificate`	The authentication certificate issued by your identity provider.
`Request Signing Certificate`	The certificate (saved in the Certificate and Key Management page in Setup) used to generate the signature on a SAML request to the identity provider when Salesforce is the service provider for a service provider-initiated SAML login. If a certificate has not been saved in the Certificate and Key Management page in Setup, Salesforce uses the global proxy certificate by default. Using a saved signing certificate provides more control over events, such as certificate expiration, than using the global proxy certificate.
`Request Signature Method`	The hashing algorithm for encrypted requests, either `RSA-SHA1` or `RSA-SHA256`.
`SAML Identity Type`	The element in a SAML assertion that contains the string that identifies a Salesforce user. Values are: **`Assertion contains User's Salesforce username`** Use this option if your identity provider passes the Salesforce username in SAML assertions.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Federated Authentication is available in: **All** Editions

Delegated Authentication is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Authentication Providers are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Modify All Data

Field	Description
	Assertion contains the Federation ID from the User object Use this option if your identity provider passes an external user identifier, for example an employee ID, in the SAML assertion to identify the user. **Assertion contains the User ID from the User object** Use this option if your identity provider passes an internal user identifier, for example a user ID from your Salesforce organization, in the SAML assertion to identify the user.
SAML Identity Location	The location in the assertion where a user should be identified. Values are: **Identity is in the NameIdentifier element of the Subject statement** The Salesforce Username or FederationIdentifier is located in the <Subject> statement of the assertion. **Identity is in an Attribute element** The Salesforce Username or FederationIdentifier is specified in an <AttributeValue>, located in the <Attribute> of the assertion.
Attribute Name	If "Identity is in an Attribute element" is selected, this contains the value of the AttributeName that is specified in <Attribute> that contains the User ID.
Attribute URI	If SAML 1.1 is the specified SAML version and "Identity is in an Attribute element" is selected, this contains the value of the AttributeNamespace that is specified in <Attribute>.
Name ID Format	If SAML 2.0 is the specified SAML version and "Identity is in an Attribute element" is selected, this contains the value for the nameid-format. Possible values include unspecified, emailAddress or persistent. All legal values can be found in the "Name Identifier Format Identifiers" section of the Assertions and Protocols SAML 2.0 specification.
Service Provider Initiated Request Binding	If you're using My Domain, chose the binding mechanism your identity provider requests for your SAML messages. Values are: **HTTP POST** HTTP POST binding sends SAML messages using base64-encoded HTML forms. **HTTP Redirect** HTTP Redirect binding sends base64-encoded and URL-encoded SAML messages within URL parameters. No matter what request binding is selected, the SAML Response will always use HTTP POST binding.
Identity Provider Login URL	For SAML 2.0 only: The URL where Salesforce sends a SAML request to start the login sequence. If you have domains deployed and a value specified for this field, login requests are usually sent to the address specified by this field. However, if you need to bypass this value (for example, your identity provider is down) add the login parameter to the query string for the login page. For example: http://mydomain.my.salesforce.com?login. Note: This field appears in Developer Edition production and sandbox organizations by default and in production organizations only if My Domain is enabled. This field does not appear in trial organizations or sandboxes linked to trial organizations.

Field	Description
`Identity Provider Logout URL`	For SAML 2.0 only: The URL to direct the user to when they click the **Logout** link in Salesforce. The default is `http://www.salesforce.com`. Note: This field appears in Developer Edition production and sandbox organizations by default and in production organizations only if My Domain is enabled. This field does not appear in trial organizations or sandboxes linked to trial organizations.
`Salesforce Login URL`	The URL associated with logging in for the Web browser single sign-on flow.
`OAuth 2.0 Token Endpoint`	For SAML 2.0 only: The ACS URL used with the API when enabling Salesforce as an identity provider in the Web single sign-on OAuth assertion flow.
`Custom Error URL`	The URL of the page users should be directed to if there's an error during SAML login. It must be a publicly accessible page, such as a public site Visualforce page. The URL can be absolute or relative.

Start, Login, and Logout URL Values

In addition to the information used during the single sign-on, your identity provider can also set the start, login, and logout pages. You can also specify these pages yourself when you configure single sign-on.

The following information might be useful to your identity provider if they are setting these pages.

- The SAML specification supports an HTML form that is used to pass the SAML assertion via HTTPS POST.
- For SAML 1.1, the SAML identity provider can embed name-value pairs in the `TARGET` field to pass this additional information to Salesforce prepended with a specially formatted URL that contains URL-encoded parameters.
- The URL for SAML 1.1 to include in the `TARGET` field is as follows: `https://saml.salesforce.com/?`
- For SAML 2.0, instead of using the `TARGET` field, the identity providers uses the `<AttributeStatement>` in the SAML assertion to specify the additional information.
- Salesforce supports the following parameters:

  Note: For SAML 1.1 these parameters must be URL-encoded. This allows the URLs, passed as values that include their own parameters, to be handled correctly. For SAML 2.0, these parameters are part of the `<AttributeStatement>`.

  - `ssoStartPage` is the page to which the user should be redirected when trying to log in with SAML. The user is directed to this page when requesting a protected resource in Salesforce, without an active session. The `ssoStartPage` should be the SAML identity provider's login page.
  - `startURL` is the URL where you want the user to be directed when sign-on completes successfully. This URL can be absolute, such as *`https://yourInstance.salesforce.com/001/o`* or it can be relative, such as *`/001/o`*. This parameter is only used in SAML 1.1. In SAML 2.0, the start URL is the page the user attempted to access before they were authenticated.
  - `logoutURL` is the URL where you want the user to be directed when they click the **Logout** link in Salesforce. The default is `http://www.salesforce.com`.

The following sample `TARGET` field is for SAML 1.1, and includes properly-encoded parameters. It passes a customized start page, as well as start and logout URLs embedded as parameter values in the query string.

```
https://saml.salesforce.com/?ssoStartPage=https%3A%2F
%2Fwww.customer.org%2Flogin%2F&startURL=%2F001%2Fo&logoutURL=http%3A%2F%2Fwww.salesforce.com
```

The following is an example of an <AttributeStatement> for SAML 2.0 that contains both ssoStartPage and logoutURL:

```
<saml:AttributeStatement>
   <saml:Attribute Name="ssoStartPage"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:anyType">
              http://www.customer.org
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="logoutURL"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">
              https://www.salesforce.com
      </saml:AttributeValue>
   </saml:Attribute>
</saml:AttributeStatement>
```

SEE ALSO:

SAML

Customize SAML Start, Error, Login, and Logout Pages

You can customize the start, error, login, and logout pages for single sign-on users using SAML 1.1 or 2.0. As part of your configuration, decide the following:

- If your identity provider uses SAML 1.1, the URL to direct the user to when single sign-on successfully completes (known as the start page). This URL can be absolute, such as *`https://yourInstance.salesforce.com/001/o`* or it can be relative, such as *`/001/o`*. This URL must be an endpoint that accepts SAML authentication requests.

  In SAML 2.0, the start page is the page the user attempted to access before they were authenticated. The SAML 2.0 start page must support Sp-init single sign-on.

  If you are using SAML 2.0, you can also use the `RelayState` parameter to control where users get redirected after a successful login.

- The single sign-on start page where Salesforce sends a SAML request to start the login sequence.

  We recommend that if you specify a single sign-on start page that you also specify a logout page. When you specify a logout page, when a user clicks logout or if a user's session expires, the user is redirected to that page. If you don't specify a logout page, the user is redirected to the general Salesforce login page.

- The URL to direct the user to when they click the Logout link in Salesforce (known as the logout page). The default is `https://login.salesforce.com`, unless MyDomain is enabled. If My Domain is enabled, the default is `https://`*`customdomain`*`.my.salesforce.com`.

For SAML 2.0, these values can be set either during the single sign-on configuration, or by your identity provider in the login URL or SAML assertion. The order of precedence is:

1. Session cookie—if you've already logged in to Salesforce and a cookie still exists, the login and logout pages specified by the session cookie are used.
2. Values passed in from the identity provider.
3. Values from the single sign-on configuration page.

If you decide not to add these values to the single sign-on configuration, share them with your identity provider. The identity provider must use these values either in the login URL or the assertion.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Federated Authentication is available in: **All** Editions

Delegated Authentication is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Authentication Providers are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view the settings:
- View Setup and Configuration

To edit the settings:
- Customize Application

  AND

  Modify All Data

You can also decide if you want users to be directed to a custom error page if there's an error during SAML login: It must be a publicly accessible page, such as a public site Visualforce page. The URL can be absolute or relative. Use this value when you configure SAML.

SEE ALSO:

SAML

Example SAML Assertions

Share the example SAML assertions with your identity provider so they can determine the format of the information Salesforce requires for successful single-sign on. The assertion must be signed according to the XML Signature specification, using RSA and either SHA-1 or SHA-256.

In addition to the general single sign-on examples for both SAML 1.1 and SAML 2.0, use the following samples for the specific feature:

- assertions for portals
- assertions for Sites
- SOAP message for delegated authentication
- assertion for just-in-time provisioning

SAML User ID type is the Salesforce username, and SAML User ID location is the `<NameIdentifier>` element in the `<Subject>` element

SAML 1.1:

```
<Subject>
      <NameIdentifier>user101@salesforce.com</NameIdentifier>
</Subject>
```

SAML 2.0:

```
<saml:Subject>
    <saml:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">user101@salesforce.com</saml:NameID>

    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml:SubjectConfirmationData NotOnOrAfter="2008-06-26T02:44:24.173Z"
Recipient="http://localhost:9000"/>
    </saml:SubjectConfirmation>
</saml:Subject>
```

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Federated Authentication is available in: **All** Editions

Delegated Authentication is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Authentication Providers are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Modify All Data

SAML User ID type is the Salesforce username, and SAML User ID location is the `<Attribute>` element

SAML 1.1:

```
<AttributeStatement>
    <Subject>
      <NameIdentifier>this value doesn't matter</NameIdentifier>
         <SubjectConfirmation>
          <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</ConfirmationMethod>

    </SubjectConfirmation>
 </Subject>
    <Attribute AttributeName="MySfdcName" AttributeNamespace="MySfdcURI">
       <AttributeValue>user101@salesforce.com</AttributeValue>
 </Attribute>
    </AttributeStatement>
```

SAML 2.0:

```
<saml:AttributeStatement>
    <saml:Attribute FriendlyName="fooAttrib" Name="SFDC_USERNAME"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
        <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">
            user101@salesforce.com
        </saml:AttributeValue>
    </saml:Attribute>
 </saml:AttributeStatement>
```

SAML User ID type is the Salesforce User object's `FederationIdentifier` field, and SAML User ID location is the `<NameIdentifier>` element in the `<Subject>` element

SAML 1.1:

```
<AttributeStatement>
   <saml:Subject>
      <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.0:assertion"
NameQualifier="www.saml_assertions.com">
         MyName
      </saml:NameIdentifier>
   </saml:Subject>
</AttributeStatement>
```

SAML 2.0:

```
<saml:Subject>
    <saml:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">MyName</saml:NameID>
    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml:SubjectConfirmationData NotOnOrAfter="2008-06-26T02:48:25.730Z"
Recipient="http://localhost:9000/"/>
    </saml:SubjectConfirmation>
</saml:Subject>
```

Note: The name identifier can be any arbitrary string, including email addresses or numeric ID strings.

SAML User ID type is theSalesforce User object's `FederationIdentifier` field, and SAML User ID location is the `<Attribute>` element

SAML 1.1:

```
<AttributeStatement>
    <Subject>
      <NameIdentifier>who cares</NameIdentifier>
         <SubjectConfirmation>
          <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</ConfirmationMethod>

    </SubjectConfirmation>
 </Subject>
    <Attribute AttributeName="MyName" AttributeNamespace="MyURI">
       <AttributeValue>user101</AttributeValue>
 </Attribute>
    </AttributeStatement>
```

SAML 2.0:

```
<saml:AttributeStatement>
    <saml:Attribute FriendlyName="fooAttrib" Name="SFDC_ATTR"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
        <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">
            user101
        </saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

SAML User ID type is the Salesforce username, and SAML User ID location is the `<NameIdentifier>` element in the `<Subject>` element

The following is a complete SAML response for SAML 2.0:

```
<samlp:Response ID="_257f9d9e9fa14962c0803903a6ccad931245264310738"
   IssueInstant="2009-06-17T18:45:10.738Z" Version="2.0">
<saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
   https://www.salesforce.com
</saml:Issuer>

<samlp:Status>
   <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>

<saml:Assertion ID="_3c39bc0fe7b13769cab2f6f45eba801b1245264310738"
   IssueInstant="2009-06-17T18:45:10.738Z" Version="2.0">
   <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
      https://www.salesforce.com
   </saml:Issuer>

   <saml:Signature>
      <saml:SignedInfo>
         <saml:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <saml:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
```

```
         <saml:Reference URI="#_3c39bc0fe7b13769cab2f6f45eba801b1245264310738">
            <saml:Transforms>
               <saml:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
               <saml:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                  <ec:InclusiveNamespaces PrefixList="ds saml xs"/>
               </saml:Transform>
            </saml:Transforms>
            <saml:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <saml:DigestValue>vzR9Hfp8d16576tEDeq/zhpmLoo=
            </saml:DigestValue>
         </saml:Reference>
      </saml:SignedInfo>
      <saml:SignatureValue>
         AzID5hhJeJlG2llUDvZswNUrlrPtR7S37QYH2W+Un1n8c6kTC
         Xr/lihEKPcA2PZt86eBntFBVDWTRlh/W3yUgGOqQBJMFOVbhK
         M/CbLHbBUVT5TcxIqvsNvIFdjIGNkf1W0SBqRKZOJ6tzxCcLo
         9dXqAyAUkqDpX5+AyltwrdCPNmncUM4dtRPjI05CL1rRaGeyX
         3kkqOL8p0vjm0fazU5tCAJLbYuYgU1LivPSahWNcpvRSlCI4e
         Pn2oiVDyrcc4et12inPMTc2lGIWWWWJyHOPSiXRSkEAIwQVjf
         Qm5cpli44Pv8FCrdGWpEE0yXsPBvDkM9jIzwCYGG2fKaLBag==
      </saml:SignatureValue>
      <saml:KeyInfo>
         <saml:X509Data>
            <saml:X509Certificate>
               MIIEATCCAumgAwIBAgIBBTANBgkqhkiG9w0BAQ0FADCBgzELM
               [Certificate truncated for readability...]
            </saml:X509Certificate>
         </saml:X509Data>
      </saml:KeyInfo>
   </saml:Signature>

   <saml:Subject>
      <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">
         saml01@salesforce.com
      </saml:NameID>

      <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml:SubjectConfirmationData NotOnOrAfter="2009-06-17T18:50:10.738Z"
         Recipient="https://login.salesforce.com"/>
      </saml:SubjectConfirmation>
   </saml:Subject>

   <saml:Conditions NotBefore="2009-06-17T18:45:10.738Z"
      NotOnOrAfter="2009-06-17T18:50:10.738Z">

      <saml:AudienceRestriction>
         <saml:Audience>https://saml.salesforce.com</saml:Audience>
      </saml:AudienceRestriction>
   </saml:Conditions>

   <saml:AuthnStatement AuthnInstant="2009-06-17T18:45:10.738Z">
      <saml:AuthnContext>
         <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
         </saml:AuthnContextClassRef>
      </saml:AuthnContext>
   </saml:AuthnStatement>

   <saml:AttributeStatement>

      <saml:Attribute Name="portal_id">
         <saml:AttributeValue xsi:type="xs:anyType">060D00000000SHZ
         </saml:AttributeValue>
      </saml:Attribute>

      <saml:Attribute Name="organization_id">
         <saml:AttributeValue xsi:type="xs:anyType">00DD0000000F7L5
         </saml:AttributeValue>
      </saml:Attribute>

      <saml:Attribute Name="ssostartpage"
         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">

         <saml:AttributeValue xsi:type="xs:anyType">
            http://www.salesforce.com/security/saml/saml20-gen.jsp
         </saml:AttributeValue>
      </saml:Attribute>

      <saml:Attribute Name="logouturl"
         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

         <saml:AttributeValue xsi:type="xs:string">
            http://www.salesforce.com/security/del_auth/SsoLogoutPage.html
         </saml:AttributeValue>
      </saml:Attribute>
   </saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
```

Sample SAML Assertions for Portals

The following shows the `portal_id` and `organization_id` attributes in a SAML assertion statement:

```
<saml:AttributeStatement>
   <saml:Attribute Name="portal_id">
      <saml:AttributeValue xsi:type="xs:anyType">060D00000000SHZ</saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="organization_id">
         <saml:AttributeValue xsi:type="xs:anyType">00DD0000000F7P5</saml:AttributeValue>

   </saml:Attribute>
</saml:AttributeStatement>
```

The following is a complete SAML assertion statement that can be used for single sign-on for portals. The organization is using federated sign-on, which is included in an attribute (see the `<saml:AttributeStatement>` in bold text in the assertion), not in the subject.

```
<samlp:Response ID="_f97faa927f54ab2c1fef230eee27cba21245264205456"
      IssueInstant="2009-06-17T18:43:25.456Z" Version="2.0">
   <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
      https://www.salesforce.com</saml:Issuer>

   <samlp:Status>
      <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
   </samlp:Status>

   <saml:Assertion ID="_f690da2480a8df7fcc1cbee5dc67dbbb1245264205456"
      IssueInstant="2009-06-17T18:45:10.738Z" Version="2.0">
      <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
         https://www.salesforce.com
      </saml:Issuer>

      <saml:Signature>
         <saml:SignedInfo>
            <saml:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
           <saml:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

            <saml:Reference URI="#_f690da2480a8df7fcc1cbee5dc67dbbb1245264205456">
               <saml:Transforms>
                  <saml:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                  <saml:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                     <ec:InclusiveNamespaces PrefixList="ds saml xs"/>
                  </saml:Transform>
               </saml:Transforms>
               <saml:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
               <saml:DigestValue>vzR9Hfp8d16576tEDeq/zhpmLoo=
               </saml:DigestValue>
            </saml:Reference>
         </saml:SignedInfo>
         <saml:SignatureValue>
            AzID5hhJeJlG2llUDvZswNUrlrPtR7S37QYH2W+Un1n8c6kTC
            Xr/lihEKPcA2PZt86eBntFBVDWTRlh/W3yUgGOqQBJMFOVbhK
            M/CbLHbBUVT5TcxIqvsNvIFdjIGNkf1W0SBqRKZOJ6tzxCcLo
            9dXqAyAUkqDpX5+AyltwrdCPNmncUM4dtRPjI05CL1rRaGeyX
            3kkqOL8p0vjm0fazU5tCAJLbYuYgU1LivPSahWNcpvRSlCI4e
            Pn2oiVDyrcc4et12inPMTc2lGIWWWWJyHOPSiXRSkEAIwQVjf
            Qm5cpli44Pv8FCrdGWpEE0yXsPBvDkM9jIzwCYGG2fKaLBag==
         </saml:SignatureValue>
         <saml:KeyInfo>
            <saml:X509Data>
               <saml:X509Certificate>
                  MIIEATCCAumgAwIBAgIBBTANBgkqhkiG9w0BAQ0FADCBgzELM
                  Certificate truncated for readability...
               </saml:X509Certificate>
            </saml:X509Data>
         </saml:KeyInfo>
      </saml:Signature>
```

```
<saml:Subject>
   <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">null

   </saml:NameID>

   <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
   <saml:SubjectConfirmationData NotOnOrAfter="2009-06-17T18:48:25.456Z"
      Recipient="https://login.salesforce.com/?saml=02HKiPoin4f49GRMsOdFmhTgi
      _0nR7BBAflopdnD3gtixujECWpxr9klAw"/>
      </saml:SubjectConfirmation>
</saml:Subject>

<saml:Conditions NotBefore="2009-06-17T18:43:25.456Z"
   NotOnOrAfter="2009-06-17T18:48:25.456Z">

   <saml:AudienceRestriction>
      <saml:Audience>https://saml.salesforce.com</saml:Audience>
   </saml:AudienceRestriction>
</saml:Conditions>

<saml:AuthnStatement AuthnInstant="2009-06-17T18:43:25.456Z">

   <saml:AuthnContext>
      <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified

      </saml:AuthnContextClassRef>
   </saml:AuthnContext>
</saml:AuthnStatement>

<saml:AttributeStatement>

   <saml:Attribute FriendlyName="Friendly Name" Name="federationId"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:string">saml_portal_user_federation_id
      </saml:AttributeValue>
      <saml:AttributeValue xsi:type="xs:string">SomeOtherValue
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="portal_id">
      <saml:AttributeValue xsi:type="xs:anyType">060D00000000SHZ
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="organization_id">
      <saml:AttributeValue xsi:type="xs:anyType">00DD0000000F7Z5
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="ssostartpage"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">

      <saml:AttributeValue xsi:type="xs:anyType">
```

```
               http://www.salesforce.com/qa/security/saml/saml20-gen.jsp
            </saml:AttributeValue>
         </saml:Attribute>

         <saml:Attribute Name="logouturl"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

            <saml:AttributeValue xsi:type="xs:string">
                http://www.salesforce.com/qa/security/del_auth/SsoLogoutPage.html
            </saml:AttributeValue>
         </saml:Attribute>
      </saml:AttributeStatement>
   </saml:Assertion>
</samlp:Response>
```

Sample SAML Assertion for Sites

The following shows the `portal_id`, `organization_id`, and `siteurl` attributes in a SAML assertion statement:

```
<saml:AttributeStatement>
   <saml:Attribute Name="portal_id">
      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:type="xs:anyType">060900000004cDk
      </saml:AttributeValue>
   </saml:Attribute>
   <saml:Attribute Name="organization_id">
      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:type="xs:anyType">00D900000008bX0
      </saml:AttributeValue></saml:Attribute>
   <saml:Attribute Name="siteurl">
      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:type="xs:anyType">https://ap1.force.com/mySuffix</saml:AttributeValue>
   </saml:Attribute>
</saml:AttributeStatement>
```

Sample SOAP Message for Delegated Authentication

As part of the delegated authentication single sign-on process, a Salesforce server makes a SOAP 1.1 request to authenticate the user who is passing in the credentials. Here is an example of this type of request. Your single sign-on Web service needs to accept this request, process it, and return a `true` or `false` response.

Sample Request

```
<?xml version="1.0" encoding="UTF-8" ?>
<soapenv:Envelope
   xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
   <soapenv:Body>
      <Authenticate xmlns="urn:authentication.soap.sforce.com">
         <username>sampleuser@sample.org</username>
         <password>myPassword99</password>
         <sourceIp>1.2.3.4</sourceIp>
      </Authenticate>
   </soapenv:Body>
</soapenv:Envelope>
```

Sample Response Message

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
   xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
   <soapenv:Body>
      <AuthenticateResult xmlns="urn:authentication.soap.sforce.com">
         <Authenticated>false</Authenticated>
      </AuthenticateResult>
   </soapenv:Body>
</soapenv:Envelope>
```

Sample SAML Assertion for Just-In-Time Provisioning

The following is a sample SAML assertion for just in time provisioning.

```
<saml:AttributeStatement>

   <saml:Attribute Name="User.Username"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">testuser@123.org
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.Phone"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">415-123-1234
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.FirstName"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">Testuser
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.LanguageLocaleKey"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">en_US
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.CompanyName"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">Salesforce.com
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.Alias"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">tlee2
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.CommunityNickname"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">tlee2
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.UserRoleId"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">000000000000000
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.Title"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">Mr.
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.LocaleSidKey"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">en_CA
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.Email"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">testuser@salesforce.com
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name=" User.FederationIdentifier"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">tlee2
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.TimeZoneSidKey"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">America/Los_Angeles
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.LastName"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">Lee
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.ProfileId"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">00ex0000001pBNL
```

```
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.IsActive"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">1
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.EmailEncodingKey"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">UTF-8
      </saml:AttributeValue>
   </saml:Attribute>

</saml:AttributeStatement>
```

SEE ALSO:

SAML

Reviewing the SAML Login History

When a user logs in to Salesforce from another application using single sign-on, SAML assertions are sent to the Salesforce login page. The assertions are checked against assertions in the authentication certificate that are specified on the Single Sign-On Settings page in Setup. If a user fails to log in, a message is written to the login history log that indicates why the login failed. In addition, the SAML Assertion Validator may be automatically populated with the invalid assertion.

To view the login history, from Setup, enter *Login History* in the Quick Find box, then select **Login History**. After viewing the login history, you may want to share the information with your identity provider.

The following are the possible failures:

Assertion Expired

An assertion's timestamp is more than five minutes old.

> Note: Salesforce does make an allowance of three minutes for clock skew. This means, in practice, that an assertion can be as much as eight minutes after the timestamp time, or three minutes before it. This amount of time may be less if the assertion's validity period is less than five minutes.

Assertion Invalid

An assertion is not valid. For example, the <Subject> element of an assertion might be missing.

Audience Invalid

The value specified in <Audience> must be https://saml.salesforce.com.

Configuration Error/Perm Disabled

Something is wrong with the SAML configuration in Salesforce. For example, the uploaded certificate might be corrupted, or the organization preference might have been turned off. To check your configuration, from Setup, enter *Single Sign-On Settings* in the Quick Find box, then select **Single Sign-On Settings**. Next, get a sample SAML assertion from your identity provider, and then click **SAML Assertion Validator**.

Issuer Mismatched

The issuer or entity ID specified in an assertion does not match the issuer specified in your Salesforce configuration.

Recipient Mismatched

The recipient specified in an assertion does not match the recipient specified in your Salesforce configuration.

Replay Detected

The same assertion ID was used more than once. Assertion IDs must be unique within an organization.

Signature Invalid

The signature in an assertion cannot be validated by the certificate in your Salesforce configuration.

Subject Confirmation Error

The <Subject> specified in the assertion does not match the SAML configuration in Salesforce.

SEE ALSO:

SAML

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Federated Authentication is available in: **All** Editions

Delegated Authentication is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Authentication Providers are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view the settings:
- View Setup and Configuration

To edit the settings:
- Customize Application

  AND

  Modify All Data

Validating SAML Settings for Single Sign-On

If your users have difficulty logging into Salesforce after you configure Salesforce for single sign-on, use the SAML Assertion Validator and the login history to validate the SAML assertions sent by your identity provider.

1. Obtain a SAML assertion from your identity provider. The assertion can be either in plain XML format or base64 encoded.

   If a user tries to log in to Salesforce and fails, the invalid SAML assertion is used to automatically populate the SAML Assertion Validator if possible.

2. From Setup, enter `Single Sign-On Settings` in the `Quick Find` box, then select **Single Sign-On Settings**, then click **SAML Assertion Validator**.
3. Enter the SAML assertion into the text box, and click **Validate**.
4. Share the results of the validation errors with your identity provider.

SEE ALSO:

SAML

Single Sign-On

Best Practices for Implementing Single Sign-On

Administrator setup guide: Single Sign-On Implementation Guide

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Federated Authentication is available in: **All** Editions

Delegated Authentication is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Authentication Providers are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Modify All Data

SAML Assertion Validation Errors

Salesforce imposes the following validity requirements on assertions:

Authentication Statement

The identity provider must include an `<AuthenticationStatement>` in the assertion.

Conditions Statement

If the assertion contains a `<Conditions>` statement, it must contain a valid timestamp.

Timestamps

The validity period specified in an assertion is honored. In addition, an assertion's timestamp must be less than five minutes old, plus or minus three minutes, regardless of the assertion's validity period setting. This allows for differences between machines. The `NotBefore` and `NotOnOrAfter` constraints must also be defined and valid.

Attribute

If your Salesforce configuration is set to `Identity is in an Attribute element`, the assertion from the identity provider must contain an `<AttributeStatement>`.

If you are using SAML 1.1, both `<AttributeName>` and `<AttributeNamespace>` are required as part of the `<AttributeStatement>`.

If you are using SAML 2.0, only `<AttributeName>` is required.

Format

The `Format` attribute of an `<Issuer>` statement must be set to `"urn:oasis:names:tc:SAML:2.0:nameid-format:entity"` or not set at all.

For example:

```
<saml:Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://www.salesforce.com</saml:Issuer>
```

The following example is also valid:

```
<saml:Issuer >https://www.salesforce.com</saml:Issuer>
```

Issuer

The issuer specified in an assertion must match the issuer specified in Salesforce.

Subject

The subject of the assertion must be resolved to be either the Salesforce username or the Federation ID of the user.

Audience

The `<Audience>` value is required and must match the `Entity ID` from the single sign-on configuration. The default value is `https://saml.salesforce.com`.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Federated Authentication is available in: **All** Editions

Delegated Authentication is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Authentication Providers are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Modify All Data

Recipient

The recipient specified in an assertion must match either the Salesforce login URL specified in the Salesforce configuration or the OAuth 2.0 token endpoint. This is a required portion of the assertion and is always verified.

Signature

A valid signature must be included in the assertion. The signature must be created using the private key associated with the certificate that was provided in the SAML configuration.

Recipient

Verifies that the recipient and organization ID received in the assertion matches the expected recipient and organization ID, as specified in the single sign-on configuration. This is an optional portion of the assertion and is only verified if it's present. For example:

```
Recipient that we found in the assertion: http://aalbert-salesforce.com:8081/
   ?saml=02HKiPoin4zeKLPYxfj3twkPsNSJF3fxsH0Jnq4vVeQr3xNkIWmZC_IVk3
Recipient that we expected based on the Single Sign-On Settings page:
   http://asmith.salesforce.com:8081/
   ?saml=EK03Almz90Cik_ig0L97.0BRme6mT4o6nzi0t_JROL6HLbdR1WVP5aQO5w
Organization Id that we expected: 00Dx0000000BQlI
Organization Id that we found based on your assertion: 00D000000000062
```

Site URL Attribute

Verifies if a valid Sites URL is provided. Values are:

- Not Provided
- Checked
- Site URL is invalid
- HTTPS is required for Site URL
- The specified Site is inactive or has exceeded its page limit

SEE ALSO:

SAML

About Just-in-Time Provisioning for SAML

With Just-in-Time provisioning, you can use a SAML assertion to create regular and portal users on the fly the first time they try to log in. This eliminates the need to create user accounts in advance. For example, if you recently added an employee to your organization, you don't need to manually create the user in Salesforce. When they log in with single sign-on, their account is automatically created for them, eliminating the time and effort with on-boarding the account. Just-in-Time provisioning works with your SAML identity provider to pass the correct user information to Salesforce in a SAML 2.0 assertion. You can both create and modify accounts this way. Because Just-in-Time provisioning uses SAML to communicate, your organization must have SAML-based single sign-on enabled.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

Benefits of Just-in-Time Provisioning

Implementing Just-in-Time provisioning can offer the following advantages to your organization.

- **Reduced Administrative Costs:** Provisioning over SAML allows customers to create accounts on-demand, as part of the single sign-on process. This greatly simplifies the integration work required in scenarios where users need to be dynamically provisioned, by combining the provisioning and single sign-on processes into a single message.

- **Increased User Adoption:** Users only need to memorize a single password to access both their main site and Salesforce. Users are more likely to use your Salesforce application on a regular basis.
- **Increased Security:** Any password policies that you have established for your corporate network are also in effect for Salesforce. In addition, sending an authentication credential that is only valid for a single use can increase security for users who have access to sensitive data.

IN THIS SECTION:

Just-in-Time Provisioning Requirements and SAML Assertion Fields

Just-in-Time Provisioning and SAML Assertion Fields for Portals

Just-in-Time Provisioning for Communities

Just-in-Time Provisioning Errors

Following are the error codes and descriptions for Just-in-Time provisioning for SAML.

SEE ALSO:

Just-in-Time Provisioning Requirements and SAML Assertion Fields

Just-in-Time Provisioning and SAML Assertion Fields for Portals

Just-in-Time Provisioning for Communities

Just-in-Time Provisioning Errors

Example SAML Assertions

Single Sign-On

Just-in-Time Provisioning Requirements and SAML Assertion Fields

Just-in-Time provisioning requires the creation of a SAML assertion. Consider the following when creating your SAML assertion.

- `Provision Version` is supported as an optional attribute. If it isn't specified, the default is 1.0. For example:

```
<saml:Attribute Name="ProvisionVersion" NameFormat=
   "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">1.0</saml:AttributeValue>
</saml:Attribute>
```

- ProfileIDs change per organization, even for standard profiles. To make it easier to find the profile name, Salesforce allows you to do a profile name lookup by passing the `ProfileName` into the `ProfileId` field.

Field Requirements for the SAML Assertion

To correctly identify which object to create in Salesforce, you must use the `User.` prefix for all fields passed in the SAML assertion. In this example, the `User.` prefix has been added to the `Username` field name.

```
<saml:Attribute
   Name="User.Username"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">testuser@123.org</saml:AttributeValue>
</saml:Attribute>
```

The following standard fields are supported. Some fields are required.

Fields	Required	Comments
`AboutMe`		
`Alias`		If not present, a default is derived from FirstName and LastName.
`CallCenter`		
`City`		
`CommunityNickname`		If not present, a default is derived from the UserName.
`CompanyName`		
`Country`		
`DefaultCurrencyIsoCode`		Derived from organization settings.
`DelegatedApproverId`		
`Department`		
`Division`		
`Email`	**Y**	For example, `User.Email=test2@salesforce.com`
`EmailEncodingKey`		If not present, a default is derived from the organization settings.
`EmployeeNumber`		
`Extension`		
`Fax`		
`FederationIdentifier` (insert only)		If present, it must match the SAML subject, or the SAML subject is taken instead. Can't be updated with SAML.
`FirstName`		
`ForecastEnabled`		
`IsActive`		
`LastName`	**Y**	
`LanguageLocaleKey`		
`LocaleSidKey`		If not present, a default is derived from the organization settings.
`Manager`		
`MobilePhone`		
`Phone`		
`ProfileId`	**Y**	For example, `User.ProfileId=Standard User`
`ReceivesAdminInfoEmails`		
`ReceivesInfoEmails`		
`State`		

Fields	Required	Comments
Street		
TimeZoneSidKey		If not present, a default is derived from the organization settings.
Title		
Username (insert only)	Y	For example, User.Username=test2@test.com. Can't update using SAML.
UserRoleId		Defaults to "no role" if blank.
Zip		

Other field requirements:

- Only text type custom fields are supported.
- Only the insert and update functions are supported for custom fields.
- When using the API for user creation, you can pass the new username into the User.Username field. You can also specify the User.FederationIdentifier if it is present. However, the Username and FederationIdentifier fields can't be updated with API.

SEE ALSO:

About Just-in-Time Provisioning for SAML

Just-in-Time Provisioning and SAML Assertion Fields for Portals

Just-in-Time Provisioning for Communities

Just-in-Time Provisioning and SAML Assertion Fields for Portals

With Just-in-Time (JIT) provisioning for portals, you can use a SAML assertion to create customer and partner portal users on the fly the first time they try to log in. This eliminates the need to create user accounts in advance. Because JIT uses SAML to communicate, your organization must have SAML-based single sign-on enabled.

Note: Starting with Summer '13, Customer Portals and partner portals are no longer available for new organizations. Existing organizations continue to have access to these portals. If you don't have a portal, but want to easily share information with your customers or partners, try Communities.

Existing organizations using Customer Portals and partner portals may continue to use their portals or transition to Communities. Contact your Salesforce Account Executive for more information.

Creating Portal Users

The Portal ID and Organization ID must be specified as part of the SAML assertion. You can find both of these on the company information page for the organization or portal. Because you can also provision regular users, the Portal ID is used to distinguish between a regular and portal JIT provisioning request. If no Portal ID is specified, then the request is treated as a JIT request for regular platform user. Here are the requirements for a creating a portal user.

- You must specify a Federation ID. If the ID belongs to an existing user account, the user account is updated. In case of an inactive user account, the user account is updated, but left inactive unless User.IsActive in the JIT assertion is set to true. If there is no user account with that Federation ID, the system creates a new user.

- If the portal isn't self-registration enabled and a default new user profile and role aren't specified, the `User.ProfileId` field must contain a valid profile name or ID associated with the portal. In addition, the `User.PortalRole` field must contain a valid portal role name or ID.

  Note: The `User.Role` must be null.

Creating and Modifying Accounts

Create or modify an account by specifying a valid `Account ID` or both the `Account.AccountNumber` and `Account.Name`.

- Matching is based on `Account.AccountNumber`. If multiple accounts are found, an error is displayed. Otherwise, the account is updated.
- If no matching account is found, one is created.
- You must specify the `Account.Owner` in the SAML assertion and ensure that the field level security for the `Account.AccountNumber` field is set to visible for this owner's profile.

Creating and Modifying Contacts

Create or modify a contact by specifying the a valid Contact ID in `User.Contact` or both the `Contact.Email` and `Contact.LastName`.

- Matching is based on `Contact.Email`. If multiple contacts are found, an error is displayed. Otherwise, the contact is updated.
- If no matching contact is found, one is created.

Supported Fields for the Portal SAML Assertion

To correctly identify which object to create in Salesforce, you must use a prefix. In the SAML assertion, use the `Account` prefix for all fields in the Account schema (for example `Account.AccountId`) and `Contact` prefix for all fields in the Contact schema. In this example, the `Contact` prefix has been added to the `Email` field name.

```
<saml:Attribute
   Name="Contact.Email"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">testuser@123.org</saml:AttributeValue>
</saml:Attribute>
```

In addition to the standard fields supported for regular SAML JIT users, these fields are supported for accounts. Some fields are required.

Fields	Required	Comments
`Billing`		Street|City|State|PostalCode|Country
`AnnualRevenue`		
`Description`		
`Fax`		
`FederationIdentifier` (insert only)	Y	If present, it must match the SAML subject or the SAML subject is taken instead. Can't be updated using SAML.
`IsCustomerPortal`		
`IsPartner`		

Fields	Required	Comments
`NumberOfEmployees`		
`Ownership`		
`Phone`		
`Portal Role`	**Y**	Use `Worker` for all portal users.
`Rating`		
`Street`		
`TickerSymbol`		
`UserRoleId`		Defaults to “no role” if blank.
`Website`		
`Zip`		

In addition to the standard fields supported for regular SAML JIT users, these fields are supported for contacts.

Fields	Required	Comments
`Birthdate`		
`CanAllowPortalSelfReg`		Name|Phone
`Department`		
`Description`		
`DoNotCall`		
`Fax`		
`HasOptedOutofEmail`		
`HasOptedOutofFax`		
`HomePhone`		
`LeadSource`		
`Mailing`		Street|City|State|PostalCode|Country
`MobilePhone`		
`Owner`		
`Other`		Street|City|State|PostalCode|Country
`OtherPhone`		
`Phone`		
`Salutation`		

Fields	Required	Comments
`Title`		

SEE ALSO:

About Just-in-Time Provisioning for SAML

Just-in-Time Provisioning Requirements and SAML Assertion Fields

Just-in-Time Provisioning for Communities

Just-in-Time Provisioning for Communities

With Just-in-Time (JIT) provisioning for Communities, you can use a SAML assertion to create customer and partner community users on the fly the first time they try to log in from an identity provider. This eliminates the need to create user accounts in advance. Because JIT uses SAML to communicate, your organization must have SAML-based single sign-on enabled. Then, you can work with the identity provider to generate the necessary SAML assertions for JIT.

SAML Single Sign-on Settings

Follow the instructions for Configure SAML Settings for Single Sign-On with `SAML Enabled`. Set the values for your configuration, as needed, and also include the following values specific to your community for JIT provisioning.

1. Check `User Provisioning Enabled`.

   Note:

   - Just-in-time provisioning requires a Federation ID in the user type. In `SAML User ID Type`, select Assertion contains the Federation ID from the User object.
   - If your identity provider previously used the Salesforce username, communicate to them that they must use the Federation ID.

2. The **Entity ID** should be unique across your organization and begin with `https`. You can't have two SAML configurations with the same **Entity ID** in one organization. Specify whether you want to use the base domain (`https://saml.salesforce.com`) or the community URL (such as `https://acme.force.com/customers`) for the **Entity ID**. You must share this information with your identity provider.

   Tip: Generally, use the community URL as the entity ID. If you are providing Salesforce to Salesforce services, you must specify the community URL.

3. In `SAML User ID Type`, select `Assertion contains the Federation ID from the User object`. If your identity provider previously used the Salesforce username, communicate to them that they must use the Federation ID.

Creating and Modifying Community Users

The SAML assertion needs the following.

- A `Recipient` URL. This is the Community Login URL from the SAML Single Sign-On Settings detail page in your organization. The URL is in the following form.

  ```
  https://<community_URL>/login?so=<orgID>
  ```

  For example, `Recipient="https://acme.force.com/customers/login?so=00DD0000000JsCM"` where `acme.force.com/customers` is the community home page and `00DD0000000JsCM` is the `Organization ID`.

If an Assertion Decryption Certificate has been uploaded to the organization's SAML Single Sign-On Settings, include the certificate ID in the URL using the `sc` parameter, such as `Recipient="https://acme.force.com/customers/login?so=00DD0000000JsCM&sc=0LE000000Dp"` where `0LE000000Dp` is the certificate ID.

- Salesforce attempts to match the `Federation ID` in the subject of the SAML assertion (or in an attribute element, depending upon how the SAML Identity Location is defined in the SAML Single Sign-On Settings) to the `FederationIdentifier` field of an existing user record.
  1. If a matching user record is found, Salesforce uses the attributes in the SAML assertion to update the specified fields.
  2. If a user with a matching user record isn't found, then Salesforce searches the contacts for a match based on the `Contact ID` (`User.Contact`) or email (`Contact.Email`). `Contact.Email` and `Contact.LastName` are both required properties when `User.Contact` is not specified, but matching is only based on `Contact.Email` when both properties exist.
     - **i.** If a matching contact record is found, Salesforce uses the attributes in the SAML assertion to update the specified contact fields, and then inserts a new user record.
     - **ii.** If a matching contact record isn't found, then Salesforce searches the accounts for a match based on the `Contact.Account` or `Account.AccountNumber` specified in the SAML assertion. `Account.AccountNumber` and `Account.Name` are both required properties when `Contact.Account` is not specified, but matching is only based on `Account.AccountNumber` when both properties exist.
       - **i.** If a matching account record is found, Salesforce inserts a new user record and updates the account records based the attributes provided in the SAML assertion.
       - **ii.** If a matching account record isn't found, Salesforce inserts new account, contact, and user records based on the attributes provided in the SAML assertion.

  In the case of an inactive user account, the user account is updated, but left inactive unless `User.IsActive` in the JIT assertion is set to true. If there is no user account with that `Federation ID`, the system creates a new user.
- If the community doesn't have self-registration enabled, and a default new user profile and role aren't specified, the `User.ProfileId` field must contain a valid profile name or ID associated with the community.

Salesforce attempts to match the `Federation ID` in the subject of the SAML assertion to the `FederationIdentifier` field of an existing user record.

> Note: Salesforce also supports custom fields on the User object in the SAML assertion. Any attribute in the assertion that starts with `User` is parsed as a custom field. For example, the attribute `User.NumberOfProductsBought__c` in the assertion is placed into the field `NumberOfProductsBought` for the provisioned user. Custom fields are not supported for Accounts or Contacts.

Supported Fields for the Community SAML Assertion

To correctly identify which object to create in Salesforce, you must use a prefix. In the SAML assertion, use the `Account` prefix for all fields in the Account schema (for example `Account.AccountId`) and `Contact` prefix for all fields in the Contact schema. In this example, the `Contact` prefix has been added to the `Email` field name.

```
<saml:Attribute
   Name="Contact.Email"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">testuser@123.org</saml:AttributeValue>
</saml:Attribute>
```

In addition to the standard fields supported for regular SAML JIT users, these fields are supported for accounts.

Fields	Required	Comments
`Billing`		Street|City|State|PostalCode|Country
`AnnualRevenue`		
`Description`		
`Fax`		
`FederationIdentifier` (insert only)	Y	If present, it must match the SAML subject or the SAML subject is taken instead. Can't be updated using SAML.
`IsCustomerPortal`		
`IsPartner`		
`NumberOfEmployees`		
`Ownership`		
`Phone`		
`Portal Role`		
`Rating`		
`Street`		
`TickerSymbol`		
`UserRoleId`		Defaults to "no role" if blank.
`Website`		
`Zip`		

In addition to the standard fields supported for regular SAML JIT users, these fields are supported for contacts.

Fields	Required	Comments
`Birthdate`		
`CanAllowPortalSelfReg`		Name|Phone
`Department`		
`Description`		
`DoNotCall`		
`Fax`		
`HasOptedOutofEmail`		
`HasOptedOutofFax`		
`HomePhone`		

Fields	Required	Comments
`LeadSource`		
`Mailing`		Street|City|State|PostalCode|Country
`MobilePhone`		
`Owner`		
`Other`		Street|City|State|PostalCode|Country
`OtherPhone`		
`Phone`		
`Salutation`		
`Title`		

SEE ALSO:

- About Just-in-Time Provisioning for SAML
- Just-in-Time Provisioning Requirements and SAML Assertion Fields

Just-in-Time Provisioning Errors

Following are the error codes and descriptions for Just-in-Time provisioning for SAML.

SAML errors are returned in the URL parameter, for example:

```
http://login.salesforce.com/identity/jit/saml-error.jsp?
ErrorCode=5&ErrorDescription=Unable+to+create+user&ErrorDetails=
INVALID_OR_NULL_FOR_RESTRICTED_PICKLIST+TimeZoneSidKey
```

Note: Salesforce redirects the user to a custom error URL if one is specified in your SAML configuration.

Error Messages

Code	Description	Error Details
1	Missing Federation Identifier	MISSING_FEDERATION_ID
2	Mis-matched Federation Identifier	MISMATCH_FEDERATION_ID
3	Invalid organization ID	INVALID_ORG_ID
4	Unable to acquire lock	USER_CREATION_FAILED_ON_UROG
5	Unable to create user	USER_CREATION_API_ERROR
6	Unable to establish admin context	ADMIN_CONTEXT_NOT_ESTABLISHED
8	Unrecognized custom field	UNRECOGNIZED_CUSTOM_FIELD
9	Unrecognized standard field	UNRECOGNIZED_STANDARD_FIELD

Code	Description	Error Details
11	License limit exceeded	LICENSE_LIMIT_EXCEEDED
12	Federation ID and username do not match	MISMATCH_FEDERATION_ID_AND_USERNAME_ATTRS
13	Unsupported provision API version	UNSUPPORTED_VERSION
14	Username change isn't allowed	USER_NAME_CHANGE_NOT_ALLOWED
15	Custom field type isn't supported	UNSUPPORTED_CUSTOM_FIELD_TYPE
16	Unable to map a unique profile ID for the given profile name	PROFILE_NAME_LOOKUP_ERROR
17	Unable to map a unique role ID for the given role name	ROLE_NAME_LOOKUP_ERROR
18	Invalid account	INVALID_ACCOUNT_ID
19	Missing account name	MISSING_ACCOUNT_NAME
20	Missing account number	MISSING_ACCOUNT_NUMBER
22	Unable to create account	ACCOUNT_CREATION_API_ERROR
23	Invalid contact	INVALID_CONTACT
24	Missing contact email	MISSING_CONTACT_EMAIL
25	Missing contact last name	MISSING_CONTACT_LAST_NAME
26	Unable to create contact	CONTACT_CREATION_API_ERROR
27	Multiple matching contacts found	MULTIPLE_CONTACTS_FOUND
28	Multiple matching accounts found	MULTIPLE_ACCOUNTS_FOUND
30	Invalid account owner	INVALID_ACCOUNT_OWNER
31	Invalid portal profile	INVALID_PORTAL_PROFILE
32	Account change is not allowed	ACCOUNT_CHANGE_NOT_ALLOWED
33	Unable to update account	ACCOUNT_UPDATE_FAILED
34	Unable to update contact	CONTACT_UPDATE_FAILED
35	Invalid standard account field value	INVALID_STANDARD_ACCOUNT_FIELD_VALUE
36	Contact change not allowed	CONTACT_CHANGE_NOT_ALLOWED
37	Invalid portal role	INVALID_PORTAL_ROLE
38	Unable to update portal role	CANNOT_UPDATE_PORTAL_ROLE
39	Invalid SAML JIT Handler class	INVALID_JIT_HANDLER
40	Invalid execution user	INVALID_EXECUTION_USER
41	Execution error	APEX_EXECUTION_ERROR

Code	Description	Error Details
42	Updating a contact with Person Account isn't supported	UNSUPPORTED_CONTACT_PERSONACCT_UPDATE

SEE ALSO:

About Just-in-Time Provisioning for SAML

Just-in-Time Provisioning and SAML Assertion Fields for Portals

External Authentication Providers

Authentication providers let your users log in to your Salesforce org using their login credentials from an external service provider. Salesforce provides authentication providers for apps that support the OpenID Connect protocol, such as Google, Facebook, Twitter, and LinkedIn. For apps that don't support OpenID Connect, Salesforce provides an Apex `Auth.AuthProviderPluginClass` abstract class to create a custom authentication provider.

You can enable users to log in to your Salesforce org using their login credentials from an external service provider such as Facebook or Janrain.

Note: Social Sign-On (Salesforce Classic) (11:33 minutes)

Learn how to configure single sign-on (SSO) and OAuth-based API access to Salesforce from other sources of user identity.

Do the following to set up a custom authentication provider for SSO.

- Configure the service provider website.
- Create a registration handler using Apex.
- Define the authentication provider in your org.

When set up is complete, the authentication provider flow is as follows.

1. The user tries to log in to Salesforce using a third-party (external) identity.
2. The login request is redirected to the external authentication provider.
3. The user follows the third-party login process and approves access.
4. The external authentication provider redirects the user to Salesforce with credentials.
5. The user is signed in to Salesforce.

Note: If users have an existing Salesforce session, after authentication with the third party, they're redirected to the page where they can approve the link to their Salesforce account.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Manage Auth. Providers

Define Your Authentication Provider

Salesforce supports the following authentication providers.

- Facebook
- Google
- LinkedIn
- Microsoft Access Control Service

- Salesforce
- Twitter
- Janrain
- Any service provider who implements the OpenID Connect protocol
- Any service provider who supports OAuth but not the OpenID Connect protocol

Add Functionality to Your Authentication Provider

You can add functionality to your authentication provider by using additional request parameters.

- Scope—Customizes the permissions requested from the third party.
- Site—Enables the provider to be used with a site.
- StartURL—Sends the user to a specified location after authentication.
- Community—Sends the user to a specific community after authentication.
- Authorization Endpoint on page 702—Sends the user to a specific endpoint for authentication (Salesforce authentication providers, only).

Create an Apex Registration Handler

You must implement a registration handler to use authentication providers for SSO. The Apex `registration handler` class must implement the `Auth.RegistrationHandler` interface, which defines two methods. Salesforce invokes the appropriate method on callback, depending on whether the user has used this provider before or not. When you create the authentication provider, you can automatically create an Apex template class for testing purposes. For more information, see RegistrationHandler in the *Force.com Apex Code Developer's Guide*.

IN THIS SECTION:

Configure a Facebook Authentication Provider

Configure a Facebook authentication provider to let your users log in to your Salesforce org using their Facebook credentials.

Configure a Google Authentication Provider

Configure Google as an authentication provider to let users log in to your Salesforce org using their Google credentials.

Configure a Janrain Authentication Provider

Configure Janrain as an authentication provider to let users log in to your Salesforce org using their Janrain credentials.

Configure a Salesforce Authentication Provider

To configure a Salesforce authentication provider, create a connected app that uses single sign-on (SSO).

Configure an OpenID Connect Authentication Provider

You can use any third-party web app that implements the server side of the OpenID Connect protocol, such as Amazon, Google, and PayPal, as an authentication provider.

Configure a Microsoft® Access Control Service Authentication Provider

You can use Microsoft Access Control Service as an authentication provider using the OAuth protocol. Authorization is typically done by a Microsoft Office 365 service like SharePoint® Online.

Configure a LinkedIn Authentication Provider

Configure LinkedIn as an authentication provider to let users log in to your Salesforce org using their LinkedIn credentials.

Configure a Twitter Authentication Provider

Configure Twitter as an authentication provider to let users log in to a Salesforce org from their Twitter account.

Use Salesforce-Managed Values in the Auth. Provider Setup Page

You can choose to let Salesforce create key values when setting up a Facebook, Salesforce, LinkedIn, Twitter, or Google authentication provider. Having Salesforce generate the key values saves you the time and effort of creating your own third-party app.

Create a Custom External Authentication Provider

Create a custom single sign-on (SSO) authentication provider to let users log in to your Salesforce org using their non-Salesforce credentials. Implement a custom external authentication provider if your OAuth app doesn't support OpenID Connect. If your app supports OpenID Connect, you can use one of the authentication providers that Salesforce provides.

Configure a Facebook Authentication Provider

Configure a Facebook authentication provider to let your users log in to your Salesforce org using their Facebook credentials.

Configuring Facebook as an authentication provider involves these high-level steps.

1. Set up a Facebook app, making Salesforce the app domain.
2. Define a Facebook authentication provider in your Salesforce org.
3. Update your Facebook app to use the Callback URL generated by Salesforce as the Facebook website URL.
4. Test the connection.

Set Up a Facebook App

Before you can configure Facebook for your Salesforce org, you must set up an app in Facebook.

Note: You can skip this step by allowing Salesforce to use its own default app. For more information, see Use Salesforce-Managed Values in the Auth. Provider Setup Page.

1. Go to the Facebook website and create an app.
2. Modify the app settings and set the Application Domain to Salesforce.
3. Note the app ID and the app secret.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To view the settings:
- View Setup and Configuration

To edit the settings:
- Customize Application

  AND

  Manage Auth. Providers

Define a Facebook Provider in Your Salesforce Org

You need the Facebook app ID and app secret to set up a Facebook provider in your Salesforce org.

Note: You can skip this step by allowing Salesforce to manage the values for you. For more information, see Use Salesforce-Managed Values in the Auth. Provider Setup Page.

1. From Setup, enter *`Auth. Providers`* in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. For provider type, select Facebook.
4. Enter a name for the provider.
5. Enter the URL suffix, which is used in the client configuration URLs. For example, if the URL suffix of your provider is MyFacebookProvider, your single sign-on (SSO) URL is similar to: `https://login.salesforce.com/auth/sso/00Dx00000000001/MyFacebookProvider`.
6. Use the Facebook app ID for the `Consumer Key` field.
7. Use the Facebook app secret for the `Consumer Secret` field.

8. Optionally, set the following fields.
   a. Enter the base URL from Facebook for the Authorize Endpoint URL. For example, `https://www.facebook.com/v2.2/dialog/oauth`. If you leave this field blank, Salesforce uses the version of the Facebook API that your app uses.

      Tip: You can add query string parameters to the base URL, if necessary. For example, to get a refresh token from Facebook for offline access, use `https://accounts.facebook.com/o/oauth2/auth?access_type=offline&approval_prompt=force`. You need the `approval_prompt` parameter to ask the user to accept the refresh action so that Facebook continues to provide refresh tokens after the first one.

   b. Enter the Token Endpoint URL from Facebook. For example, `https://www.facebook.com/v2.2/dialog/oauth`. If you leave this field blank, Salesforce uses the version of the Facebook API that your app uses.
   c. Enter the User Info Endpoint URL to change the values requested from Facebook's profile API. See https://developers.facebook.com/docs/facebook-login/permissions/v2.0#reference-public_profile for more information on fields. The requested fields must correspond to the requested scopes. If you leave this field blank, Salesforce uses the version of the Facebook API that your app uses.
   d. `Default Scopes` to send along with the request to the authorization endpoint. Otherwise, the hardcoded defaults for the provider type are used (see Facebook's developer documentation for these defaults).

      For more information, see Use the Scope Parameter.

   e. `Custom Error URL` for the provider to use to report any errors.
   f. `Custom Logout URL` to provide a specific destination for users after they log out, if they authenticated using the SSO flow. Use this field to direct users to a branded logout page or destination other than the default Salesforce logout page. The URL must be fully qualified with an `http` or `https` prefix, such as `https://acme.my.salesforce.com`.
   g. Select an existing Apex class as the `Registration Handler` class. Or click **Automatically create a registration handler template** to create an Apex class template for the registration handler. Edit this class later, and modify the default content before using it.

      Note: A `Registration Handler` class is required for Salesforce to generate the SSO initialization URL.

   h. For `Execute Registration As`, select the user that runs the Apex handler class. The user must have the "Manage Users" permission. A user is required regardless of whether you're specifying an existing registration handler class or creating one from the template.
   i. To use a portal with your provider, select the portal from the Portal dropdown list.
   j. Use the `Icon URL` field to add a path to an icon to display as a button on the login page for a community. This icon applies to a community only. It doesn't appear on the login page for your Salesforce org or domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

      Specify a path to your own image, or copy the URL for one of our sample icons into the field.

9. Click **Save**.

Note the generated Auth. Provider Id value. You use it with the `Auth.AuthToken` Apex class.

Several client configuration URLs are generated after defining the authentication provider.

- Test-Only Initialization URL—Salesforce admins use this URL to ensure that the third-party provider is set up correctly. The admin opens this URL in a browser, signs in to the third party, and is redirected back to Salesforce with a map of attributes.

- Single Sign-On Initialization URL—Use this URL to perform SSO into Salesforce from a third party using its third-party credentials. The user opens this URL in a browser and logs in to the third party. The third party either creates a user or updates an existing user. Then the third party signs the user into Salesforce as that user.
- Existing User Linking URL—Use this URL to link existing Salesforce users to a third-party account. The user opens this URL in a browser, signs in to the third party, signs in to Salesforce, and approves the link.
- Oauth-Only Initialization URL—Use this URL to obtain OAuth access tokens for a third party. Users must authenticate with Salesforce for the third-party service to get a token. This flow doesn't provide for future SSO functionality.
- Callback URL—Use the callback URL for the endpoint that the authentication provider calls back to for configuration. The authentication provider must redirect to the callback URL with information for each client configuration URL.

Client configuration URLs support additional request parameters that enable you to direct users to log in to specific sites, obtain customized permissions from the third party, or go to a specific location after authenticating.

Update Your Facebook App

After defining the Facebook authentication provider in your Salesforce org, go back to Facebook and update your app to use the Callback URL as the Facebook Website Site URL.

Test the SSO Connection

In a browser, open the Test-Only Initialization URL on the Auth. Provider detail page. It redirects you to Facebook and asks you to sign in. You're then asked to authorize your app. After you authorize, you're redirected back to Salesforce.

SEE ALSO:

Use Request Parameters with Client Configuration URLs

External Authentication Providers

Configure a Google Authentication Provider

Configure Google as an authentication provider to let users log in to your Salesforce org using their Google credentials.

Complete these steps to configure Google as an authentication provider.

1. Set up a Google app, making Salesforce the application domain.
2. Define a Google authentication provider in your Salesforce org.
3. Update your Google app to use the callback URL generated by Salesforce as the Google website site URL.
4. Test the connection.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To view the settings:
- View Setup and Configuration

To edit the settings:
- Customize Application

  AND

  Manage Auth. Providers

Set Up a Google App

Before you can configure Google for your Salesforce org, you must set up an app in Google.

Note: You can skip this step by allowing Salesforce to use its own default app. For more information, see Use Salesforce-Managed Values in the Auth. Provider Setup Page.

1. Go to the Google website and create a new app.
2. Modify the app settings and set the application domain to Salesforce.
3. Note the app ID and the app secret.

Define a Google Provider in Your Salesforce Org

You need the Google app ID and app secret to set up a Google provider in your Salesforce org.

Note: You can skip this step by allowing Salesforce to manage the values for you. For more information, see Use Salesforce-Managed Values in the Auth. Provider Setup Page.

1. From Setup, enter `Auth. Providers` in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. For provider type, select Google.
4. Enter a name for the provider.
5. Enter the URL suffix, which is used in the client configuration URLs. For example, if the URL suffix of your provider is MyGoogleProvider, your SSO URL is similar to: `https://login.salesforce.com/auth/sso/00Dx00000000001/MyGoogleProvider`.
6. Use the Google app ID for the `Consumer Key` field.
7. Use the Google app secret for the `Consumer Secret` field.
8. Optionally, set the following fields.
   a. `Authorize Endpoint URL`—Specify the base authorization URL from Google. For example, `https://accounts.google.com/o/oauth2/authorize`. The URL must start with `https://accounts.google.com/o/oauth2`.

      Tip: You can add query string parameters to the base URL, if necessary. For example, to get a refresh token from Google for offline access, use `https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force`. You need the `approval_prompt` parameter to ask the user to accept the refresh action so that Google continues to provide refresh tokens after the first one.

   b. `Token Endpoint URL`—Specify the OAuth token URL from Google. For example, `https://accounts.google.com/o/oauth2/accessToken`. The URL must start with `https://accounts.google.com/o/oauth2`.
   c. `User Info Endpoint URL`—Change the values requested from Google's profile API. The URL must start with `https://www.googleapis.com/oauth2/`.
   d. `Default Scopes`—Send with the request to the authorization endpoint. Otherwise, the hardcoded defaults for the provider type are used. For the defaults, see Google's developer documentation.

      For more information, see Use the Scope Parameter.

   e. `Custom Error URL`—Specify a URL for the provider to report errors.
   f. `Custom Logout URL` to provide a specific destination for users after they log out, if they authenticated using the SSO flow. Use this field to direct users to a branded logout page or destination other than the default Salesforce logout page. The URL must be fully qualified with an `http` or `https` prefix, such as `https://acme.my.salesforce.com`.
   g. Select an existing Apex class as the `Registration Handler` class. Or click **Automatically create a registration handler template** to create an Apex class template for the registration handler. Edit this class later, and modify the default content before using it.

      Note: A `Registration Handler` class is required for Salesforce to generate the SSO initialization URL.

h. For `Execute Registration As`, select the user that runs the Apex handler class. The user must have the "Manage Users" permission. A user is required regardless of whether you're specifying an existing registration handler class or creating one from the template.

i. To use a portal with your provider, select the portal from the Portal list.

j. Use the `Icon URL` field to add a path to an icon to display as a button on the login page for a community. This icon applies to a community only. It doesn't appear on the login page for your Salesforce org or domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

   Specify a path to your own image, or copy the URL for one of our sample icons into the field.

9. Click **Save**.

Note the generated `Auth. Provider Id` value. You use it with the `Auth.AuthToken` Apex class.

Several client configuration URLs are generated after defining the authentication provider.

- Test-Only Initialization URL—Admins use this URL to ensure that the third-party provider is set up correctly. The admin opens this URL in a browser, signs in to the third party, and is redirected back to Salesforce with a map of attributes.
- Single Sign-On Initialization URL—Use this URL to perform single sign-on (SSO) into Salesforce from a third party (using third-party credentials). The user opens this URL in a browser and signs in to the third party. The third party either creates a user or updates an existing user. Then the third party signs the user into Salesforce as that user.
- Existing User Linking URL—Use this URL to link existing Salesforce users to a third-party account. The user opens this URL in a browser, signs in to the third party, signs in to Salesforce, and approves the link.
- Oauth-Only Initialization URL—Use this URL to obtain OAuth access tokens for a third party. Users must authenticate with Salesforce for the third-party service to get a token;. This flow doesn't provide for future SSO functionality.
- Callback URL—Use the callback URL for the endpoint that the authentication provider calls back to for configuration. The authentication provider redirects to the callback URL with information for each client configuration URL.

Client configuration URLs support other request parameters that enable you to direct users to log in to specific sites, obtain customized permissions from a third party, or go to a location after authenticating.

Update Your Google App

After defining the Google authentication provider in your Salesforce org, go back to Google and update your app to use the callback URL as the Google website site URL.

Test the SSO Connection

In a browser, open the Test-Only Initialization URL on the Auth. Provider Setup page. It redirects you to Google and asks you to sign in. You're then asked to authorize your app. After you authorize, you're redirected to Salesforce.

Configure a Janrain Authentication Provider

Configure Janrain as an authentication provider to let users log in to your Salesforce org using their Janrain credentials.

Setting up a Janrain authentication provider is slightly different from setting up other providers. You don't use the single sign-on initialization URL that you obtain after registering your provider with Salesforce to start the flow. Instead, you use Janrain's login widget that's deployed on your site.

To set up your Janrain provider:

1. Register your app with Janrain and get an `apiKey`.
2. Define the Janrain authentication provider in your Salesforce org.
3. Get the login widget code from Janrain.
4. Set up a site that calls the login widget code in your Salesforce org.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To view the settings:
- View Setup and Configuration

To edit the settings:
- Customize Application

  AND

  Manage Auth. Providers

Register Your App

Sign up for a Janrain account from the Janrain website. After you have your Janrain account, you need the `apiKey`.

1. Select **Deployment** > **Sign-in for Web** > **Handle Tokens**.
2. Copy the `apiKey`. You need the key later when creating the Janrain provider in your Salesforce org.
3. Add `Salesforce` to the Janrain domain whitelist in your Janrain account at **Deployment** > **Application Settings** > **Domain Whitelist**.

Define the Janrain Provider in Your Salesforce Org

You need the Janrain API key to create a Janrain provider in your Salesforce org.

1. From Setup, enter *`Auth. Providers`* in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. For provider type, select Janrain.
4. Enter a name for the provider.
5. Enter the URL suffix, which is used in the callback URL. For example, if the URL suffix of your provider is MyJanrainProvider, your callback URL is similar to `https://login.salesforce.com/services/authcallback/00D300000007CvvEAE/MyJanrainProvider`.
6. Use the Janrain `apiKey` value for the `Consumer Secret`.
7. Optionally, enter a custom error URL for the provider to use to report errors.
8. Optionally, enter a custom logout URL to provide a destination for users after they log out if they authenticated using the single sign-on (SSO) flow. Use this field to direct users to a branded logout page or destination other than the default Salesforce logout page. The URL must be fully qualified with an http or https prefix, such as `https://acme.my.salesforce.com`.
9. Select an existing Apex class as the `Registration Handler` class. Or click **Automatically create a registration handler template** to create an Apex class template for the registration handler. Edit this class later, and modify the default content before using it.

   Note: A `Registration Handler` class is required for Salesforce to generate the single sign-on initialization URL.

10. For `Execute Registration As`, select the user that runs the Apex handler class. The user must have the "Manage Users" permission. A user is required regardless of whether you're specifying an existing registration handler class or creating one from the template.
11. To use a portal with your provider, select the portal from the Portal dropdown list.
12. Use the `Icon URL` field to add a path to an icon to display as a button on the login page for a community. This icon applies to a community only. It doesn't appear on the login page for your Salesforce org or domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

    Specify a path to your own image, or copy the URL for one of our sample icons into the field.

13. Click **Save**.

Note the value of the generated callback URL. You need this URL to complete the Janrain setup.

Several client configuration parameters are available after configuring Janrain as the authentication provider. Use them for the `flowtype` value in the callback URL with your Janrain login widget.

- `test`—Make sure that the third-party provider is set up correctly. The admin configures a Janrain widget to use `flowtype=test`, signs in to the third party, and is redirected back to Salesforce with a map of attributes.
- `link`—Link existing Salesforce users to a third-party account . The user goes to a page with a Janrain widget configured to use `flowtype=link`, signs in to the third party, signs in to Salesforce, and approves the link.
- `sso`—Perform SSO into Salesforce from a third party (using third-party credentials). The user goes to a page with a Janrain widget configured to use `flowtype=sso`, and signs in to the third party. The third party either creates a user or updates an existing user. Then the third party signs the user into Salesforce as that user.

Client configuration URLs support additional request parameters that enable you to direct users to log in to specific sites, obtain customized permissions from the third party, or go to a specific location after authenticating.

Get the Login Widget Code from Janrain

You need to get the login widget code from Janrain for your Salesforce org.

1. From your Janrain account, select **Application** > **Sign-in for Web** > **Get the Code**.
2. Enter the callback URL value from your Janrain provider information in your Salesforce org along with the query parameter `flowtype=sso` as the token URL. For example,

    ```
    https://login.salesforce.com/services/authcallback/00DD##############/JanrainApp?flowtype=sso
    ```

    For a domain created with My Domain, replace `login.salesforce.com` with your My Domain name.

    For a community, add the `community` parameter and pass it to the login widget as the token URL. For example,

    ```
    janrain.settings.tokenUrl='https://login.salesforce.com/services/authcallback/00DD##############/JanrainApp'
    +'?flowtype=sso&community='+encodeURIComponent('https://acme.force.com/customers');
    ```

Create a Site to Call the Login Widget

1. Enable Sites.
2. Create a page and copy the login widget code to the page.

3. Create a site and specify the page that you created as the home page for the site.

SEE ALSO:

Use Request Parameters with Client Configuration URLs

External Authentication Providers

Configure a Salesforce Authentication Provider

To configure a Salesforce authentication provider, create a connected app that uses single sign-on (SSO).

Configuring a Salesforce authentication provider involves these high-level steps.

1. Create a Connected App.
2. Define the Salesforce authentication provider in your org.
3. Test the connection.

Create a Connected App

You can create a connected app from either Lightning Experience or Salesforce Classic.

In Lightning Experience, from Setup, enter *App* in the `Quick Find` box, select **App Manager**, then click **New Connected App**.

In Salesforce Classic, from Setup, enter *Apps* in the `Quick Find` box, select **Apps**. Then, under the Connected Apps section, click **New**.

After you finish creating a connected app, note the values from the `Consumer Key` and `Consumer Secret` fields.

Note: You can skip this step by allowing Salesforce to use its own default app. For more information, see Use Salesforce-Managed Values in the Auth. Provider Setup Page.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Manage Auth. Providers

Define the Salesforce Authentication Provider in Your Org

To set up the authentication provider in your org, you need the values from the `Consumer Key` and `Consumer Secret` fields of the connected app definition.

Note: You can skip this step by allowing Salesforce to manage the values for you. For more information, see Use Salesforce-Managed Values in the Auth. Provider Setup Page.

1. From Setup, enter *Auth. Providers* in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. For provider type, select Salesforce.
4. Enter a name for the provider.
5. Enter the URL suffix, which is used in the client configuration URLs. For example, if the URL suffix of your provider is MySFDCProvider, your SSO URL is similar to `https://login.salesforce.com/auth/sso/00Dx00000000001/MySFDCProvider`.
6. Paste the consumer key value from the connected app definition into the `Consumer Key` field.
7. Paste the consumer secret value from the connected app definition into the `Consumer Secret` field.
8. Optionally, set the following fields.

a. `Authorize Endpoint URL` to specify an OAuth authorization URL.

   For the `Authorize Endpoint URL`, the host name can include a sandbox or custom domain name (created using My Domain), but the URL must end in `.salesforce.com`, and the path must end in `/services/oauth2/authorize`. For example, `https://login.salesforce.com/services/oauth2/authorize`.

b. `Token Endpoint URL` to specify an OAuth token URL.

   For the `Token Endpoint URL`, the host name can include a sandbox or custom domain name (created using My Domain), but the URL must end in `.salesforce.com`, and the path must end in `/services/oauth2/token`. For example, `https://login.salesforce.com/services/oauth2/token`.

c. `Default Scopes` to send along with the request to the authorization endpoint. Otherwise, the hardcoded default is used.

   For more information, see Use the Scope Parameter.

d. `Include identity organization's organization ID for third-party account linkage`. This option doesn't appear if the authentication provider was created after the Winter '15 release. Before Winter '15, the destination org couldn't differentiate between users with the same user ID on different orgs, for example, between a production and sandbox org. As of Winter '15, user identities contain the org ID, so this option doesn't appear. For older authentication providers, enable this option to keep the identities separate in the destination org. However, if you enable this option, your users must reapprove all their third-party links. The links are listed in the Third-Party Account Links section of a user's detail page.

e. `Custom Error URL` for the provider to use to report any errors.

f. `Custom Logout URL` to provide a specific destination for users after they log out, if they authenticated using the SSO flow. Use this field to direct users to a branded logout page or destination other than the default Salesforce logout page. The URL must be fully qualified with an `http` or `https` prefix, such as `https://acme.my.salesforce.com`.

9. Select an existing Apex class as the `Registration Handler` class. Or click **Automatically create a registration handler template** to create an Apex class template for the registration handler. Edit this class later, and modify the default content before using it.

   Note: A `Registration Handler` class is required for Salesforce to generate the SSO initialization URL.

10. For `Execute Registration As`, select the user that runs the Apex handler class. The user must have the "Manage Users" permission. A user is required regardless of whether you're specifying an existing registration handler class or creating one from the template.

11. To use a portal with your provider, select the portal from the Portal dropdown list.

12. Use the `Icon URL` field to add a path to an icon to display as a button on the login page for a community. This icon applies to a community only. It doesn't appear on the login page for your Salesforce org or domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

    Specify a path to your own image, or copy the URL for one of our sample icons into the field.

13. Click **Save**.

    Note the value of the Client Configuration URLs. You need the callback URL to complete the last step. Use the Test-Only initialization URL to check your configuration. Also note the `Auth. Provider Id` value because you use it with the `Auth.AuthToken` Apex class.

14. Return to the connected app definition that you created earlier from Setup. Paste the callback URL value from the authentication provider into the `Callback URL` field.

Several client configuration URLs are generated after defining the authentication provider.

- Test-Only Initialization URL—Salesforce admins use this URL to ensure that the third-party provider is set up correctly. The admin opens this URL in a browser, signs in to the third party, and is redirected back to Salesforce with a map of attributes.
- Single Sign-On Initialization URL—Use this URL to perform SSO into Salesforce from a third party using its third-party credentials. The user opens this URL in a browser and logs in to the third party. The third party either creates a user or updates an existing user. Then the third party signs the user into Salesforce as that user.
- Existing User Linking URL—Use this URL to link existing Salesforce users to a third-party account. The user opens this URL in a browser, signs in to the third party, signs in to Salesforce, and approves the link.
- Oauth-Only Initialization URL—Use this URL to obtain OAuth access tokens for a third party. Users must authenticate with Salesforce for the third-party service to get a token. This flow doesn't provide for future SSO functionality.
- Callback URL—Use the callback URL for the endpoint that the authentication provider calls back to for configuration. The authentication provider must redirect to the callback URL with information for each client configuration URL.

Client configuration URLs support additional request parameters that enable you to direct users to log in to specific sites, obtain customized permissions from the third party, or go to a specific location after authenticating.

Test the SSO Connection

In a browser, open the Test-Only Initialization URL on the Auth. Provider detail page. It redirects you to the authentication provider and asks you to sign in. You're then asked to authorize your app. After you authorize, you're redirected to Salesforce.

SEE ALSO:

Use Request Parameters with Client Configuration URLs

External Authentication Providers

Configure an OpenID Connect Authentication Provider

You can use any third-party web app that implements the server side of the OpenID Connect protocol, such as Amazon, Google, and PayPal, as an authentication provider.

Complete these steps to configure an OpenID authentication provider.

1. Register your app, making Salesforce the app domain.
2. Define an OpenID Connect authentication provider in your Salesforce org.
3. Update your app to use the callback URL generated by Salesforce.
4. Test the connection.

Register an OpenID Connect App

Before you can configure a web app for your Salesforce org, you must register it with your service provider. The process varies depending on the service provider. For example, to register a Google app, Create an OAuth 2.0 Client ID.

1. Register your app on your service provider's website.
2. Modify the app settings and set the app domain (or Home Page URL) to Salesforce.
3. From the provider's documentation, get the client ID, client secret, authorize endpoint URL, token endpoint URL, and the user info endpoint URL. Here are some common OpenID Connect service providers.
    - Amazon

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To view the settings:
- View Setup and Configuration

To edit the settings:
- Customize Application

  AND

  Manage Auth. Providers

- Google
- PayPal

Define an OpenID Connect Provider in Your Salesforce Org

1. From Setup, enter `Auth. Providers` in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. For provider type, select **OpenID Connect**.
4. Enter a name for the provider.
5. Enter the URL suffix, which is used in the client configuration URLs. For example, if the URL suffix of your provider is MyOpenIDConnectProvider, your single sign-on URL is similar to: `https://login.salesforce.com/auth/sso/00Dx00000000001/MyOpenIDConnectProvider`.
6. Use the client ID from your provider for the `Consumer Key` field.
7. Use the client secret from your provider for the `Consumer Secret` field.
8. Enter the base URL from your provider for the `Authorize Endpoint URL`.

   Tip: You can add query string parameters to the base URL, if necessary. For example, to get a refresh token from Google for offline access, use `https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force`. You need the `approval_prompt` parameter to ask the user to accept the refresh action so that Google continues to provide refresh tokens after the first one.

9. Enter the token endpoint URL from your provider.
10. Optionally, set the following fields.
    a. `User Info Endpoint URL` from your provider.
    b. `Token Issuer`. This value identifies the source of the authentication token in the form `https: URL`. If this value is specified, the provider must include an `id_token` value in the response to a token request. The `id_token` value isn't required for a refresh token flow (but will be validated by Salesforce if provided).
    c. `Default Scopes` to send along with the request to the authorization endpoint. Otherwise, the hardcoded defaults for the provider type are used. See the OpenID Connect developer documentation for these defaults.

    For more information, see Use the Scope Parameter.

11. Optionally, select **Send access token in header** to have the token sent in a header instead of a query string.
12. Optionally, set the following fields.
    a. `Custom Error URL` for the provider to use to report any errors.
    b. `Custom Logout URL` to provide a specific destination for users after they log out, if they authenticated using the SSO flow. Use this field to direct users to a branded logout page or destination other than the default Salesforce logout page. The URL must be fully qualified with an `http` or `https` prefix, such as `https://acme.my.salesforce.com`.
    c. Select an existing Apex class as the `Registration Handler` class. Or click **Automatically create a registration handler template** to create an Apex class template for the registration handler. Edit this class later, and modify the default content before using it.

    Note: A `Registration Handler` class is required for Salesforce to generate the single sign-on initialization URL.

d. For `Execute Registration As`, select the user that runs the Apex handler class. The user must have the "Manage Users" permission. A user is required regardless of whether you're specifying an existing registration handler class or creating one from the template.

e. To use a portal with your provider, select the portal from the Portal dropdown list.

f. Use the `Icon URL` field to add a path to an icon to display as a button on the login page for a community. This icon applies to a community only. It doesn't appear on the login page for your Salesforce org or domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

Specify a path to your own image, or copy the URL for one of our sample icons into the field.

13. Click **Save**.

Be sure to note the generated Auth. Provider Id value. You must use it with the `Auth.AuthToken` Apex class.

Several client configuration URLs are generated after defining the authentication provider.

- Test-Only Initialization URL—Salesforce admins use this URL to ensure that the third-party provider is set up correctly. The admin opens this URL in a browser, signs in to the third party, and is redirected back to Salesforce with a map of attributes.
- Single Sign-On Initialization URL—Use this URL to perform SSO into Salesforce from a third party using its third-party credentials. The user opens this URL in a browser and logs in to the third party. The third party either creates a user or updates an existing user. Then the third party signs the user into Salesforce as that user.
- Existing User Linking URL—Use this URL to link existing Salesforce users to a third-party account. The user opens this URL in a browser, signs in to the third party, signs in to Salesforce, and approves the link.
- Oauth-Only Initialization URL—Use this URL to obtain OAuth access tokens for a third party. Users must authenticate with Salesforce for the third-party service to get a token. This flow doesn't provide for future SSO functionality.
- Callback URL—Use the callback URL for the endpoint that the authentication provider calls back to for configuration. The authentication provider must redirect to the callback URL with information for each client configuration URL.

Client configuration URLs support additional request parameters that enable you to direct users to log in to specific sites, obtain customized permissions from the third party, or go to a specific location after authenticating.

Update Your OpenID Connect App

After defining the authentication provider in your Salesforce org, go back to your provider and update your app's callback URL. For Google apps, the callback URL is called the Authorized Redirect URI. For PayPal, it's called the Return URL.

Test the SSO Connection

In a browser, open the Test-Only Initialization URL on the Auth. Provider Setup page. It redirects you to your provider's service and asks you to sign in. You're then asked to authorize your app. After you authorize, you're redirected back to Salesforce.

Configure a Microsoft® Access Control Service Authentication Provider

You can use Microsoft Access Control Service as an authentication provider using the OAuth protocol. Authorization is typically done by a Microsoft Office 365 service like SharePoint® Online.

Salesforce supports authentication from a Microsoft Access Control Service using only OAuth. Single sign-on (SSO) authentication from a Microsoft authentication provider is not supported.

Complete these steps to configure a Microsoft Access Control Service authentication provider.

1. Define a Microsoft Access Control Service authentication provider in your Salesforce org.
2. Register your app with Microsoft, making Salesforce the application domain.
3. Edit your Microsoft Access Control Service authentication provider details in Salesforce to use the consumer key and consumer secret generated when you registered your app with Microsoft.
4. Test the connection.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Manage Auth. Providers

Define a Microsoft Access Control Service Authentication Provider in Your Salesforce Org

Before you can register an app in SharePoint Online or the Microsoft Seller Dashboard, you need the callback URL that redirects the authorized user to Salesforce.

1. From 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.
4. Enter a name for the provider.
5. Enter the URL suffix, which is used in the client configuration URLs. For example, if the URL suffix of your provider is MyMicrosoftACSProvider, your callback URL is similar to:

   ```
   https://login.salesforce.com/services/authcallback/00Dx00000000001/MyMicrosoftACSProvider
   ```

6. Enter a placeholder value for the consumer key field. You edit this value after your app is registered with Microsoft.
7. Enter a placeholder value for the consumer secret field You edit this value after your app is registered with Microsoft.
8. Enter the base URL from your provider for the Authorize Endpoint URL. For example, SharePoint Online uses the following form.

   ```
   https://<sharepoint online host name>/_layouts/15/OAuthAuthorize.aspx
   ```

9. Enter the Token Endpoint URL in the following form.

   ```
   https://accounts.accesscontrol.windows.net/<tenant>/tokens/OAuth/2?resource=<sender ID>/<sharepoint online host name>@<tenant>
   ```

   - <tenant> is the Office 365 tenant name ending with `.onmicrosoft.com` or the corresponding tenant globally unique identifier (GUID).
   - <sender ID> is the identifier for the sender of the token. For example, SharePoint uses `00000003-0000-0ff1-ce00-000000000000`

10. Optionally, set the following fields.
    - `Default Scopes` to send along with the request to the authorization endpoint. See http://msdn.microsoft.com/en-us/library/jj687470.aspx#Scope for more information about scopes for SharePoint Online. Or Use the Scope Parameter for more information about using scopes with Salesforce.
    - `Custom Error URL` for the provider to use to report any errors.

- `Custom Logout URL` to provide a specific destination for users after they log out, if they authenticated using the SSO flow. Use this field to direct users to a branded logout page or destination other than the default Salesforce logout page. The URL must be fully qualified with an `http` or `https` prefix, such as `https://acme.my.salesforce.com`.
- To use a portal with your provider, select the portal from the Portal dropdown list. If you have a portal set up for your org, this option can redirect the login request to the portal login page. Otherwise, leave as None.
- Use the `Icon URL` field to add a path to an icon to display as a button on the login page for a community. This icon applies to a community only. It doesn't appear on the login page for your Salesforce org or domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

  Specify a path to your own image, or copy the URL for one of our sample icons into the field.

11. Click **Save**.

Note the generated Auth. Provider Id value. You can use it with the `Auth.AuthToken` Apex class.

Several client configuration URLs are generated after defining the authentication provider.

- Test-Only Initialization URL—Admins use this URL to ensure that the third-party provider is set up correctly. The admin opens this URL in a browser, signs in to the third party, and is redirected back to Salesforce with a map of attributes.
- Oauth-Only Initialization URL—Use this URL to obtain OAuth access tokens for a third party. Users must authenticate with Salesforce for the third-party service to get a token. This flow doesn't provide for future SSO functionality.
- Callback URL—Use the callback URL for the endpoint that the authentication provider calls back to for configuration. The authentication provider has to redirect to the callback URL with information for each client configuration URL.

Client configuration URLs support additional request parameters that enable you to direct users to log in to specific sites, obtain customized permissions from the third party, or go to a specific location after authenticating.

Register Your App with Microsoft

Before you can configure an app for your Salesforce org, you must get an app identity using one of the options provided by Microsoft. See Guidelines for registering apps for SharePoint 2013 for details about registering a remote app for SharePoint.

1. Register your app using one of the options provided by Microsoft.
2. Modify the app settings and set the redirect URI to the authentication provider's callback URL.
3. Note the client ID and client secret.
4. Click **Save**.

Edit Your Microsoft Access Control Service Authentication Provider Details

After registering your app with Microsoft, go back to your Microsoft Access Control Service authentication provider details, and update the consumer key and consumer secret with the values provided by Microsoft.

1. From Setup, enter *`Auth. Providers`* in the `Quick Find` box, then select **Auth. Providers**.
2. Click **Edit** next to the name of your Microsoft Access Control Service authentication provider.
3. In the `Consumer Key` field, enter the Microsoft client ID.
4. In the `Consumer Secret` field, enter the Microsoft client secret.

Test the Connection

In a browser, open the Test-Only Initialization URL on the Auth. Provider Setup page. It redirects you to Microsoft and asks you to sign in. You're then asked to authorize your app. After you authorize, you're redirected to Salesforce.

Configure a LinkedIn Authentication Provider

Configure LinkedIn as an authentication provider to let users log in to your Salesforce org using their LinkedIn credentials.

Complete these steps to configure LinkedIn as an authentication provider.

1. Decide which scopes (user details) to get from LinkedIn.
2. Set up a LinkedIn app.
3. Define a LinkedIn provider in your Salesforce org and establish a registration handler.
4. Edit the registration handler.
5. Update your LinkedIn app to use the callback URL generated by Salesforce as an entry in the LinkedIn `OAuth 2.0 Redirect URLs`.
6. Test the single sign-on (SSO) connection.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To view the settings:
- View Setup and Configuration

To edit the settings:
- Customize Application

  AND

  Manage Auth. Providers

Decide Which Scopes (User Details) to Get from LinkedIn

Scopes determine the information you get from LinkedIn about a user during the authorization process. You can request basic information, such as username and a photo URL, or you can get more specific information, such as an address, phone number, and contact list. The user approves the exchange of information before it's given.

When you set up LinkedIn as an authentication provider, you can set the scopes in three different places: in the LinkedIn app settings, in the Salesforce Auth. Provider settings, or in a query to LinkedIn's user info endpoint using field selectors. Consider the following as you decide where to specify the scopes and the values to use.

- You can leave scope value blank in the LinkedIn and Salesforce settings. The default value is r_basicprofile, which provides only the most basic user information as defined by LinkedIn.
- Salesforce requires the email address for users.
- Refer to the LinkedIn Authentication documentation for a list of supported values and their meaning, or the LinkedIn Field Selectors page for information about requesting scopes using a URL.
- If you set the default scopes in the Salesforce authentication provider settings, that value overrides the value in the LinkedIn app settings.
- Separate multiple scope values in the LinkedIn app settings or the Salesforce authentication provider settings with a space, for example, *`r_basicprofile r_emailaddress`*.
- If you use LinkedIn Field Selectors with a URL, separate multiple values with a comma, for example, `https://api.linkedin.com/v1/people/~:(id,formatted-name,first-name,last-name,public-profile-url,email-address)`.

Set Up a LinkedIn App

Before you can configure LinkedIn for your Salesforce org, set up an app in LinkedIn.

Note: You can skip this step by allowing Salesforce to use its own default app. For more information, see Use Salesforce-Managed Values in the Auth. Provider Setup Page.

1. Sign in to your developer account for the LinkedIn website.
2. Click the username at the top and select **API Keys**.
3. Click **Add New Application**.
4. Enter the app settings.

5. Note the API key and secret key. You need them later to create a LinkedIn provider in your Salesforce org.
6. Optionally, enter a LinkedIn supported scope value or several space-separated values.

   For more information about using scopes with LinkedIn, see Decide Which Scopes (User Details) to Get from LinkedIn.

Define a LinkedIn Provider in Your Salesforce Org

You need the LinkedIn API key and secret key to set up a LinkedIn provider in your Salesforce org.

Note: You can skip this step by allowing Salesforce to manage the values for you. For more information, see Use Salesforce-Managed Values in the Auth. Provider Setup Page.

1. From Setup, enter *Auth. Providers* in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. For provider type, select LinkedIn.
4. Enter a name for the provider.
5. Enter the URL suffix, which is used in the client configuration URLs. For example, if the URL suffix of your provider is MyLinkedInProvider, your SSO URL is similar to:

   ```
   https://login.salesforce.com/services/sso/00Dx00000000001/MyLinkedInProvider
   ```
6. Use the LinkedIN API key for the `Consumer Key` field.
7. Use the LinkedIn secret key for the `Consumer Secret` field.
8. Optionally, set the following fields.
   a. `Authorize Endpoint URL` to enter the base authorization URL from LinkedIn. For example, `https://www.linkedin.com/uas/oauth2/authorization/auth`. The URL must start with *`https://www.linkedin.com/uas/oauth2/authorization`*.

      Tip: You can add query string parameters to the base URL, if necessary. For example, to get a refresh token from LinkedIn for offline access, use `https://accounts.linkedin.com/o/oauth2/auth?access_type=offline&approval_prompt=force`. You need the `approval_prompt` parameter to ask the user to accept the refresh action so that LinkedIn continues to provide refresh tokens after the first one.

   b. `Token Endpoint URL` to enter the OAuth token URL from LinkedIn. For example, `https://www.linked.com/uas/oauth2/accessToken/token`. The URL must start with *`https://www.linkedin.com/uas/oauth2/accessToken`*.

   c. `User Info Endpoint URL` to change the values requested from LinkedIn's profile API. For more information, see https://developer.linkedin.com/documents/profile-fields. The URL must start with *`https://api.linkedin.com/v1/people/~`*, and the requested fields must correspond to requested scopes.

   d. `Default Scopes` to enter a supported value or several space-separated values that represent the information you get from LinkedIn. For more information, see Decide Which Scopes (User Details) to Get from LinkedIn.

   e. `Custom Error URL` for the provider to use to report any errors.

   f. `Custom Logout URL` to provide a specific destination for users after they log out, if they authenticated using the SSO flow. Use this field to direct users to a branded logout page or destination other than the default Salesforce logout page. The URL must be fully qualified with an `http` or `https` prefix, such as `https://acme.my.salesforce.com`.

g. Select an existing Apex class as the `Registration Handler` class. Or click **Automatically create a registration handler template** to create an Apex class template for the registration handler. Edit this class later, and modify the default content before using it.

   Note: A `Registration Handler` class is required for Salesforce to generate the single sign-on initialization URL.

h. For `Execute Registration As`, select the user that runs the Apex handler class. The user must have the "Manage Users" permission. A user is required regardless of whether you're specifying an existing registration handler class or creating one from the template.

i. To use a portal for LinkedIn users, select the portal from the Portal dropdown list.

9. Use the `Icon URL` field to add a path to an icon to display as a button on the login page for a community. This icon applies to a community only. It doesn't appear on the login page for your Salesforce org or domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

   Specify a path to your own image, or copy the URL for one of our sample icons into the field.

10. Click **Save**.

Several client configuration URLs are generated after defining the authentication provider.

- Test-Only Initialization URL—Admins use this URL to ensure that the third-party provider is set up correctly. The admin opens this URL in a browser, signs in to the third party, and is redirected back to Salesforce with a map of attributes.
- Single Sign-On Initialization URL—Use this URL to perform SSO into Salesforce from a third party (using third-party credentials). The user opens this URL in a browser and signs in to the third party. The third party either creates a user or updates an existing user. Then the third party signs the user into Salesforce as that user.
- Existing User Linking URL—Use this URL to link existing Salesforce users to a third-party account. The user opens this URL in a browser, signs in to the third party, signs in to Salesforce, and approves the link.
- Oauth-Only Initialization URL—Use this URL to obtain OAuth access tokens for a third party. Users must authenticate with Salesforce for the third-party service to get a token. This flow does not provide for future SSO functionality.
- Callback URL—Use the callback URL for the endpoint that the authentication provider calls back to for configuration. The authentication provider has to redirect to the callback URL with information for each client configuration URL.

Client configuration URLs support additional request parameters that enable you to direct users to log in to specific sites, obtain customized permissions from the third party, or go to a specific location after authenticating.

Edit the Registration Handler

1. From Setup, enter *`Apex Classes`* in the `Quick Find` box, then select **Apex Classes**.
2. Edit the auto-created Apex registration handler (or the existing registration handler if you had one) to map fields between LinkedIn and Salesforce

   Note: The default profile query for LinkedIn only retrieves the following fields: first-name, last-name, headline, profile URL. The default registration handler requires email. Either remove the email requirement from the registration handler or change the desired scopes in Decide Which Scopes (User Details) to Get from LinkedIn to include the email address, and any other fields you want in the registration handler.

   Here's an example Apex registration handler specifically for a LinkedIn app as the authentication provider. This registration handler assumes that the requested scopes include r_basicprofile and r_emailaddress. It also assumes that the users are logging in to a customer portal.

```
//TODO:This auto-generated class includes the basics for a Registration
//Handler class. You will need to customize it to ensure it meets your needs and
```

```
//the data provided by the third party.
global class LinkedInRegHandler implements Auth.RegistrationHandler {
    //Creates a Standard salesforce or a community user
    global User createUser(Id portalId, Auth.UserData data) {
        if (data.attributeMap.containsKey('sfdc_networkid')) {
            //We have a community id, so create a user with community access
            //TODO: Get an actual account
            Account a =[SELECT Id FROM account WHERE name = 'LinkedIn Account'];
            Contact c = new Contact();
            c.accountId = a.Id;
            c.email = data.email;
            c.firstName = data.firstName;
            c.lastName = data.lastName;
            insert(c);
            //TODO: Customize the username and profile. Also check that the username
            //doesn't already exist and possibly ensure there are enough org licenses
            //to create a user. Must be 80 characters or less.
            User u = new User();
            Profile p =[SELECT Id FROM profile WHERE name = 'Customer Portal Manager'];

            u.username = data.firstName + '@sfdc.linkedin.com';
            u.email = data.email;
            u.lastName = data.lastName;
            u.firstName = data.firstName;
            String alias = data.firstName;
            //Alias must be 8 characters or less
            if (alias.length() > 8) {
                alias = alias.substring(0, 8);
            }
            u.alias = alias;
            u.languagelocalekey = UserInfo.getLocale();
            u.localesidkey = UserInfo.getLocale();
            u.emailEncodingKey = 'UTF-8';
            u.timeZoneSidKey = 'America/Los_Angeles';
            u.profileId = p.Id;
            u.contactId = c.Id;
            return u;
        } else {
            //This is not a community, so create a regular standard user
            User u = new User();
            Profile p =[SELECT Id FROM profile WHERE name = 'Standard User'];
            //TODO: Customize the username. Also check that the username doesn't
            //already exist and possibly ensure there are enough org licenses
            //to create a user. Must be 80 characters or less
            u.username = data.firstName + '@salesforce.com';
            u.email = data.email;
            u.lastName = data.lastName;
            u.firstName = data.firstName;
            String alias = data.firstName;
            //Alias must be 8 characters or less
            if (alias.length() > 8) {
                alias = alias.substring(0, 8);
            }
            u.alias = alias;
            u.languagelocalekey = UserInfo.getLocale();
            u.localesidkey = UserInfo.getLocale();
            u.emailEncodingKey = 'UTF-8';
            u.timeZoneSidKey = 'America/Los_Angeles';
            u.profileId = p.Id;
            return u;
        }
    }
    //Updates the user's first and last name
    global void updateUser(Id userId, Id portalId, Auth.UserData data) {
        User u = new User(id = userId);
        u.lastName = data.lastName;
        u.firstName = data.firstName;
        update(u);
    }
}
```

See the RegistrationHandler Interface documentation for more information and examples.

Update Your LinkedIn App

After you define the LinkedIn authentication provider in your Salesforce org, go back to LinkedIn. Update your app to use the Salesforce-generated callback URL as the LinkedIn `OAuth 2.0 Redirect URLs` value.

Test the SSO Connection

In a browser, open the Test-Only Initialization URL on the Auth. Provider Setup page. It redirects you to LinkedIn and asks you to sign in. You're then asked to authorize your app. After you authorize, you're redirected to Salesforce.

Configure a Twitter Authentication Provider

Configure Twitter as an authentication provider to let users log in to a Salesforce org from their Twitter account.

Complete these steps to configure Twitter as an authentication provider.

1. Set up a Twitter app.
2. Define a Twitter provider in your Salesforce org, and establish a registration handler.
3. Edit the registration handler.
4. Update your Twitter app to use the callback URL generated by Salesforce as an entry in the Twitter app settings.
5. Test the single sign-on (SSO) connection.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To view the settings:
- View Setup and Configuration

To edit the settings:
- Customize Application

  AND

  Manage Auth. Providers

Set Up a Twitter App

Before you can configure Twitter for your Salesforce org, set up an app in Twitter.

Note: You can skip this step by allowing Salesforce to use its own default app. For more information, see Use Salesforce-Managed Values in the Auth. Provider Setup Page.

1. Sign in to your developer account for the Twitter website.
2. Click the user icon at the top and select **My Applications** (or go to apps.twitter.com).

3. Click **Create New App**.
4. Enter the app settings.
5. In the API Keys, note the API key and API secret. You need them later to create a Twitter provider in your Salesforce org.

Define a Twitter Provider in Your Salesforce Org

You need the Twitter API key and API secret from your Twitter app to set up a Twitter provider in your Salesforce org.

Note: You can skip this step by allowing Salesforce to manage the values for you. For more information, see Use Salesforce-Managed Values in the Auth. Provider Setup Page.

1. From Setup, enter *Auth. Providers* in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. For provider type, select Twitter.
4. Enter a name for the provider.
5. Enter the URL suffix, which is used in the client configuration URLs. For example, if the URL suffix of your provider is MyTwitterProvider, your SSO URL is similar to:

   `https://login.salesforce.com/services/sso/00Dx00000000001/MyTwitterProvider`

6. Use the API key from Twitter for the `Consumer Key` field.
7. Use the API secret from Twitter for the `Consumer Secret` field.
8. Optionally, set the following fields.
   a. `Custom Error URL` for the provider to use to report any errors.
   b. `Custom Logout URL` to provide a specific destination for users after they log out, if they authenticated using the SSO flow. Use this field to direct users to a branded logout page or destination other than the default Salesforce logout page. The URL must be fully qualified with an `http` or `https` prefix, such as `https://acme.my.salesforce.com`.
   c. Select an existing Apex class as the `Registration Handler` class. Or click **Automatically create a registration handler template** to create an Apex class template for the registration handler. Edit this class later, and modify the default content before using it.

      Note: A `Registration Handler` class is required for Salesforce to generate the SSO initialization URL.

   d. For `Execute Registration As`, select the user that runs the Apex handler class. The user must have the "Manage Users" permission. A user is required regardless of whether you're specifying an existing registration handler class or creating one from the template.
   e. To use a portal for Twitter users, select the portal from the Portal dropdown list.
   f. Use the `Icon URL` field to add a path to an icon to display as a button on the login page for a community. This icon applies to a community only. It doesn't appear on the login page for your Salesforce org or domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

      Specify a path to your own image, or copy the URL for one of our sample icons into the field.

9. Click **Save**.

Several client configuration URLs are generated after defining the authentication provider.

- Test-Only Initialization URL—Admins use this URL to ensure that the third-party provider is set up correctly. The admin opens this URL in a browser, signs in to the third party, and is redirected back to Salesforce with a map of attributes.

- Single Sign-On Initialization URL—Use this URL to perform SSO into Salesforce from a third party (using third-party credentials). The user opens this URL in a browser and signs in to the third party. The third party either creates a user or updates an existing user. Then the third party signs the user into Salesforce as that user.
- Existing User Linking URL—Use this URL to link existing Salesforce users to a third-party account. The user opens this URL in a browser, signs in to the third party, signs in to Salesforce, and approves the link.
- Callback URL—Use the callback URL for the endpoint that the authentication provider calls back to for configuration. The authentication provider has to redirect to the Callback URL with information for each client configuration URL.

Client configuration URLs support additional request parameters that enable you to direct users to log in to specific sites, obtain customized permissions from the third party, or go to a specific location after authenticating.

Edit the Registration Handler

1. From Setup, enter *`Apex Classes`* in the `Quick Find` box, then select **Apex Classes**.
2. Edit the auto-created Apex registration handler (or the existing registration handler if you had one) to map fields between Twitter and Salesforce.

   Here's an example Apex registration handler that specifies the Twitter app as the authentication provider.

```
global class MyTwitterRegHandler implements Auth.RegistrationHandler{

global User createUser(Id portalId, Auth.UserData data)
{
    if(data.attributeMap.containsKey('sfdc_networkid'))
    {
        // Create communities user
        Account a = [SELECT Id FROM account WHERE name='Twitter Account']; // Make sure
 this account exists

        Contact c = new Contact();
        c.accountId = a.Id;
        c.email = 'temp@CHANGE-ME.com';
        c.firstName = data.fullname.split(' ')[0];
        c.lastName  = data.fullname.split(' ')[1];
        insert(c);

        User u = new User();
        Profile p = [SELECT Id FROM profile WHERE name='Customer Portal Manager'];
        u.username = data.username + '@sfdc-portal-twitter.com';
        u.email = 'temp@CHANGE-ME.com';
        u.firstName = data.fullname.split(' ')[0];
        u.lastName = data.fullname.split(' ')[1];
        String alias = data.fullname;

        //Alias must be 8 characters or less
        if(alias.length() > 8) {
            alias = alias.substring(0, 8);
    }

    u.alias = alias;
    u.languagelocalekey = 'en_US';
    u.localesidkey = 'en_US';
    u.emailEncodingKey = 'UTF-8';
    u.timeZoneSidKey = 'America/Los_Angeles';
    u.profileId = p.Id;
    u.contactId = c.Id;
    return u;
} else {
    // Create Standard SFDC user
    User u = new User();
    Profile p = [SELECT Id FROM profile WHERE name='Standard User'];
    u.username = data.username + '@sfdc-twitter.com';
    u.email = 'temp@CHANGE-ME.com';
    u.firstName = data.fullname.split(' ')[0];
    u.lastName = data.fullname.split(' ')[1];
    String alias = data.fullname;
    if(alias.length() > 8)
        alias = alias.substring(0, 8);

    u.alias = alias;
    u.languagelocalekey = 'en_US';
    u.localesidkey = 'en_US';
    u.emailEncodingKey = 'UTF-8';
    u.timeZoneSidKey = 'America/Los_Angeles';
    u.profileId = p.Id;
    return u;
}
}

global void updateUser(Id userId, Id portalId, Auth.UserData data)
{
    User u = new User(id=userId);
    u.firstName = data.fullname.split(' ')[0];
    u.lastName = data.fullname.split(' ')[1];
    String alias = data.fullname;
    if(alias.length() > 8)
        alias = alias.substring(0, 8);

    u.alias = alias;
    update(u);
}
}
```

See the RegistrationHandler Interface documentation for more information and examples.

Update Your Twitter App

After you define the Twitter authentication provider in your Salesforce org, go back to Twitter and update your app to use the Salesforce-generated callback URL as the callback URL value in your Twitter app settings.

Note: In your Twitter app, make sure that you select **Allow this app to be used to Sign In with Twitter**.

Test the SSO Connection

In a browser, open the Test-Only Initialization URL on the Auth. Provider detail page. It redirects you to Twitter and asks you to sign in. You're then asked to authorize your app. After you authorize, you're redirected to Salesforce.

Use Salesforce-Managed Values in the Auth. Provider Setup Page

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Manage Auth. Providers

You can choose to let Salesforce create key values when setting up a Facebook, Salesforce, LinkedIn, Twitter, or Google authentication provider. Having Salesforce generate the key values saves you the time and effort of creating your own third-party app.

To use Salesforce-managed values, leave the following fields blank if they show up in your Auth. Provider Setup page.

- `Consumer Key`
- `Consumer Secret`
- `Authorize Endpoint URL`
- `Token Endpoint URL`
- `User Info Endpoint URL`
- `Default Scopes`

Note: Specifying a value for any of the above fields implies that you're using your own connected app. In this case, you must specify values for the consumer key and consumer secret.

Example: Suppose that you want to set up single sign-on (SSO) using a LinkedIn authentication provider to enable login to Salesforce with LinkedIn credentials. You can skip creating a LinkedIn app if you use Salesforce-created values in the Auth. Provider Setup page. Next, you define the LinkedIn authentication provider in your org and test the connection using the procedure in Configure a LinkedIn Authentication Provider.

Create a Custom External Authentication Provider

EDITIONS

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

Create a custom single sign-on (SSO) authentication provider to let users log in to your Salesforce org using their non-Salesforce credentials. Implement a custom external authentication provider if your OAuth app doesn't support OpenID Connect. If your app supports OpenID Connect, you can use one of the authentication providers that Salesforce provides.

1. Set up an account with your chosen authentication provider.
2. Create your custom metadata types, and select the custom fields that you want your admins to populate during setup.
3. Build the matching Apex classes and methods for your chosen metadata types. Then use these classes to implement a custom authentication provider by extending the abstract class `Auth.AuthProviderPluginClass`.
4. Configure your new metadata on the Auth. Provider Setup page.
5. Update your app to use the Callback URL generated by Salesforce.
6. Test the connection.

Set Up Your Account

Before you can configure the external authentication provider plug-in for your Salesforce org, set up an account with your chosen external authentication provider.

1. Go to your authentication provider's site and create an app.
2. Modify the app settings and set the Application Domain to Salesforce.
3. Note the app ID and app secret, if required by your external authentication provider.

Create Your Custom Metadata Types

When you have an account, create the custom metadata types for your Salesforce org required by your external authentication provider.

1. From Setup, enter `metadata` in the `Quick Find` box, then select **Custom Metadata Types**.
2. Click **New Custom Metadata Type**.
3. Enter a label name and plural label name for your custom metadata, and click **Save**.
4. Under the Custom Fields section, click **New** and select the custom fields you that your authentication provider requires. For example, if the authentication provider requires an app ID or app secret, create fields with labels like "Consumer Key" or "Consumer Secret."

Note: You're prompted to enter details for each field type, such as label, description, and Help text. You can choose to make these fields required.

Build Your Apex Classes and Methods

To create a custom authentication provider for SSO, create a class that extends the `Auth.AuthProviderPluginClass` abstract class. This class allows you to store the custom configuration for your authentication provider and handle its authentication protocols. It also creates the name for your external authentication provider and displays this name in the list of available authentication providers.

1. From Setup, enter `apex classes` in the search field, and select **Apex Classes**.
2. Click **New**.
3. In the field provided, create an Apex class and method.
   a. Extend the `Auth.AuthProviderPluginClass` class.
   b. For the `return` string on the `getCustomMetadataType` method, enter the API name listed on your newly created custom metadata.

Note: For information about the classes and methods that this plug-in requires, see the Auth Namespace section of the Force.com Apex Code Developer's Guide.

Configure Your Authentication Provider

You need your authentication provider's app ID and app secret to set up your custom provider in your Salesforce org.

1. From Setup, enter `Auth. Providers` in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. For the provider type, select your custom authentication provider.
4. Enter a name for the provider.
5. Enter the URL suffix, which is used in the client configuration URL. For example, if your provider's URL is MyAwesomeProvider, your SSO URL is similar to `https://login.salesforce.com/auth/sso/00Dx00000000001/MyAwesomeProvider`.
6. Enter your information in the custom fields you created.
7. Select an existing Apex class as the `Registration Handler` class. Or click **Automatically create a registration handler template** to create an Apex class template for the registration handler. Edit this class later, and modify the default content before using it.

   Note: A `Registration Handler` class is required for Salesforce to generate the SSO initialization URL.

8. For Execute Registration As, select the user that runs the Apex handler class. The user must have the "Manage Users" permission. A user is required regardless of whether you're specifying an existing registration handler class or creating one from the template. This field is required for all custom authentication providers.
9. Use the `Icon URL` field to add a path to an icon to display as a button on the login page for a community. This icon applies to a community only. It doesn't appear on the login page for your Salesforce org or domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

   Specify a path to your own image, or copy the URL for one of our sample icons into the field.
10. Click **Save**.

Note the generated authentication provider ID. You use it with the `Auth.AuthToken` Apex class.

Several client configuration URLs are generated after defining the authentication provider.

- Test-Only Initialization URL—Use to ensure that the third-party provider is set up correctly. The admin opens this URL in a browser, signs in to the third party, and is redirected back to Salesforce with a map of attributes.
- Single Sign-On Initialization URL—Use to initialize SSO into Salesforce from a third party (using third-party credentials). The user opens this URL in a browser and signs in to the third party. The third party either creates a user or updates an existing user. Then the third party signs the user into Salesforce as that user.
- Existing User Linking URL—Use to link existing Salesforce users to a third-party account. The user opens this URL in a browser, signs in to the third party, signs in to Salesforce, and approves the link.
- Oauth-Only Initialization URL—Use to obtain OAuth access tokens for a third party. Users must authenticate with Salesforce for the third-party service to get a token. This flow doesn't provide for future SSO functionality.
- Callback URL—Use as the endpoint that the authentication provider calls back to for configuration. The authentication provider redirects to the callback URL with information for each client configuration URL.

Client configuration URLs support other request parameters that enable you to direct users to log in to specific sites, obtain customized permissions from a third party, or go to a location after authenticating.

Update Your External Authentication Provider

After defining your authentication provider in your Salesforce org, go back to your external authentication provider's site and update your app to use the callback URL as your custom authentication provider's website URL.

Test the SSO Connection

In a browser, open the Test-Only Initialization URL on the Auth. Provider Setup page. It redirects you to your provider's site and asks you to sign in. You're then asked to authorize your app. After you authorize, you're redirected back to Salesforce.

SEE ALSO:

Authentication Configuration Endpoint

Using Frontdoor.jsp to Log Into Salesforce

You can use frontdoor.jsp to give users access to Salesforce from a custom Web interface, such as a remote access Force.com site, using their existing session ID and the server URL.

To authenticate users with frontdoor.jsp, you must parse the session ID (not just the 15-character or 18-character ID) and the instance or domain from the serverUrl of the LoginResult returned from the SOAP API login() call. We recommend passing these values to frontdoor.jsp through a form that uses a `POST` request.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

For example, the following form posts the current session ID to frontdoor.jsp.

```
<form method="POST" action="https://domain name/secur/frontdoor.jsp">
<input type="hidden" name="sid"
      value="full_sessionID_value"
      />
<input type="submit" name="login" value="Log In" /></form>
```

In this example, *`domain_name`* is the domain of the serverURL (that is, *`yourInstance`*.salesforce.com or *`myDomain`*.my.salesforce.com, depending on whether My Domain is enabled).

You can also send the values as URL parameters, but this approach is not as secure as a `POST` request because it exposes the session ID in the URL.

```
https://domain_name/secur/frontdoor.jsp?sid=full_sessionID_value
&retURL=optional_relative_url_to_open
```

Full Session ID

You can obtain the full session ID from:

- The `access_token` from an OAuth authentication

  Tip: One of the scopes specified when you create a connected app must be web or full.

- The Apex `UserInfo.getSessionId()`

The session ID returned using the Visualforce `{!GETSESSIONID()}` can't be used on frontdoor.jsp.

Note: Not all session types are supported with frontdoor.jsp, such as community API sessions. For these sessions, consider using SAML for single sign-on, instead.

Relative URL to Open

You can optionally include a URL-encoded relative path to redirect users to the Salesforce user interface or a particular record, object, report, or Visualforce page (for example, `/apex/MyVisualforcePage`).

Use Request Parameters with Client Configuration URLs

Add functionality to your authentication provider with request parameters. For example, you can use these parameters to direct users to log in to specific sites, get customized permissions from the third party, or go to a specific location after authenticating.

Add the request parameters to client configuration URLs. These parameters are generated after you defined your authentication provider.

- Test-Only Initialization URL
- Single Sign-On Initialization URL
- Existing User Linking URL
- Callback URL

Append any of these parameters to your URL as needed. For Janrain providers, append them to the appropriate callback URL.

- Scope—Customizes the permissions requested from the third party.
- Site—Enables the provider to be used with a site.
- StartURL—Sends the user to a specified location after authentication.
- Community—Sends the user to a specific community after authentication.
- Authorization Endpoint on page 702—Sends the user to a specific endpoint for authentication (Salesforce authentication providers, only).

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Manage Auth. Providers

IN THIS SECTION:

Use the Scope Parameter

Customize the permissions requested from a third party, like Facebook or Janrain, so that the returned access token has additional permissions.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To view the settings:
- View Setup and Configuration

To edit the settings:
- Customize Application

  AND

  Manage Auth. Providers

You can customize requests to a third party to receive access tokens with additional permissions. Then you use `Auth.AuthToken` methods to retrieve the access token that was granted so you can use those permissions with the third party.

The default scopes vary depending on the third party, but usually do not allow access to much more than basic user information. Every provider type (Open ID Connect, Facebook, Salesforce, and others), has a set of default scopes it sends along with the request to the authorization endpoint. For example, Salesforce's default scope is `id`.

You can send scopes in a space-delimited string. The space-delimited string of requested scopes is sent as-is to the third party, and overrides the default permissions requested by authentication providers.

Janrain does not use this parameter; additional permissions must be configured within Janrain.

Example: The following is an example of a `scope` parameter requesting the Salesforce scopes `api` and `web`, added to the `Single Sign-On Initialization URL`, where:

- *`orgID`* is your Auth. Provider ID
- *`URLsuffix`* is the value you specified when you defined the authentication provider

```
https://login.salesforce.com/services/auth/sso/orgID/URLsuffix?scope=id%20api%20web
```

Valid scopes vary depending on the third party; refer to your individual third-party documentation. For example, Salesforce scopes are:

Value	Description
`api`	Allows access to the current, logged-in user's account using APIs, such as REST API and Bulk API. This value also includes `chatter_api`, which allows access to Chatter REST API resources.
`chatter_api`	Allows access to Chatter REST API resources only.
`custom_permissions`	Allows access to the custom permissions in an organization associated with the connected app, and shows whether the current user has each permission enabled.
`full`	Allows access to all data accessible by the logged-in user, and encompasses all other scopes. `full` does not return a refresh token. You must explicitly request the `refresh_token` scope to get a refresh token.
`id`	Allows access to the identity URL service. You can request `profile`, `email`, `address`, or `phone`, individually to get the same result as using `id`; they are all synonymous.
`openid`	Allows access to the current, logged in user's unique identifier for OpenID Connect apps. The `openid` scope can be used in the OAuth 2.0 user-agent flow and the OAuth 2.0 Web server authentication flow to get back a signed ID token conforming to the OpenID Connect specifications in addition to the access token.
`refresh_token`	Allows a refresh token to be returned if you are eligible to receive one. This lets the app interact with the user's data while the user is offline, and is synonymous with requesting `offline_access`.
`visualforce`	Allows access to Visualforce pages.

Value	Description
`web`	Allows the ability to use the `access_token` on the Web. This also includes `visualforce`, allowing access to Visualforce pages.

SEE ALSO:

Use Request Parameters with Client Configuration URLs

Using the Site Parameter

Use your authentication provider to log into a site or link to a sites user.

To use your provider with a site, you need to do the following:

- Enable the provider to be used with a site
- Ensure the site is configured to use the same portal
- Add the site-specific login URL information to the appropriate client configuration URL, such as the `Single Sign-On Initialization URL`, using the `site` parameter

Example: You create the site login Visualforce page, or specify the default page, when you create the site. An example site login URL is: `https%3A%2F%2Fmysite.force.com%2FSiteLogin`.

The following is an example of a site-login URL added to the `Single Sign-On Initialization URL`, using the `site` parameter, where:

- *`orgID`* is your Auth. Provider ID
- *`URLsuffix`* is the value you specified when you defined the authentication provider

```
https://login.salesforce.com/services/auth/sso/orgID/URLsuffix?site=https%3A%2F%2Fmysite.force.com%2FSiteLogin
```

If you don't specify a `site` parameter, the user proceeds either to a standard portal (if set up for a portal) or the standard application (if not).

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Manage Auth. Providers

SEE ALSO:

Use Request Parameters with Client Configuration URLs

Using the StartURL Parameter

Send your user to a specific location after authenticating or linking.

To direct your users to a specific location after authenticating, you need to specify a URL with the `startURL` request parameter. This URL must be a relative URL; passing an absolute URL results in an error. If you don't add `startURL`, the user is sent to either `/home/home.jsp` (for a portal or standard application) or to the default sites page (for a site) after authentication completes.

Example: For example, with a `Single Sign-On Initialization URL`, the user is sent to this location after being logged in. For an `Existing User Linking URL`, the "Continue to Salesforce" link on the confirmation page leads to this page.

The following is an example of a `startURL` parameter added to the `Single Sign-On Initialization URL`, where:

- *`orgID`* is your Auth. Provider ID
- *`URLsuffix`* is the value you specified when you defined the authentication provider

```
https://login.salesforce.com/services/auth/sso/orgID/URLsuffix?startURL=%2F005x00000000001%3Fnoredirect%3D1
```

SEE ALSO:

Use Request Parameters with Client Configuration URLs

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Manage Auth. Providers

Using the Community URL Parameter

Send your user to a specific Community after authenticating.

To direct your users to a specific community after authenticating, you need to specify a URL with the `community` request parameter. If you don't add the parameter, the user is sent to either `/home/home.jsp` (for a portal or standard application) or to the default sites page (for a site) after authentication completes.

Example: For example, with a `Single Sign-On Initialization URL`, the user is sent to this location after being logged in. For an `Existing User Linking URL`, the "Continue to Salesforce" link on the confirmation page leads to this page.

The following is an example of a `community` parameter added to the `Single Sign-On Initialization URL`, where:

- *`orgID`* is your Auth. Provider ID
- *`URLsuffix`* is the value you specified when you defined the authentication provider

```
https://login.salesforce.com/services/auth/sso/orgID/URLsuffix?community=https://acme.force.com/support
```

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Manage Auth. Providers

Using the Authorization Endpoint Parameter

Send your user to a specific authorization endpoint.

You can add a `provAuthorizeEndpointHost` parameter to a Salesforce authentication provider URL to direct users to an authorization endpoint for a provided domain, such as a custom domain created using My Domain. Providing an authorization endpoint lets you take advantage of features like session discovery during authorization. This parameter is only available for Salesforce authentication providers, and cannot be used to send users to an authorization page outside of a Salesforce domain.

To direct your users to a specific Salesforce authorization endpoint, you need to specify a URL with the `provAuthorizeEndpointHost` request parameter and a valid `https` host. Query strings appended to the host URL are ignored. However, you can specify a community path.

Example: The following is an example of a `provAuthorizeEndpointHost` parameter added to the authentication provider URL:

- *`orgID`* is your Auth. Provider ID
- *`URLsuffix`* is the value you specified when you defined the authentication provider

```
https://login.salesforce.com/services/auth/sso/orgID/
URLsuffix?provAuthorizeEndpointHost=https%3A%2F%2Fmydomain.my.salesforce.com
```

The following is an example of a `provAuthorizeEndpointHost` directed to a community URL

```
https://login.salesforce.com/services/auth/sso/orgID/
URLsuffix?provAuthorizeEndpointHost=https%3A%2F%2Fmycommunity.force.com%2Fbilling
```

If an authorization endpoint is not provided, Salesforce uses the default authorization endpoint for the authorization provider. If no default is set for the authorization provider, Salesforce uses the endpoint for login.salesforce.com.

The authorization endpoint does not change the token endpoint, which continues to be the configured or default host. For example, if the authorization endpoint is a sandbox instance, and your provider is set to use a production token endpoint, the flow fails, because authorization was granted by the sandbox instance, only.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Manage Auth. Providers

Identity Providers and Service Providers

An *identity provider* is a trusted provider that lets you use single sign-on (SSO) to access other websites. A *service provider* is a website that hosts apps. You can enable Salesforce as an identity provider and define one or more service providers. Your users can then access other apps directly from Salesforce using SSO. SSO can be a great help to your users—instead of having to remember many passwords, they only have to remember one.

Before you can enable Salesforce as an identity provider, you must set up a subdomain with My Domain.

Enabling Salesforce as an identity provider requires a Salesforce certificate and key pair that's signed by an external certificate authority (CA-signed) or self-signed. If you haven't generated a Salesforce certificate and key pair, one is created for you when you enable Salesforce as an identity provider. Optionally, you can pick an existing generated certificate or create one yourself.

Salesforce uses the SAML 2.0 standard for SSO and generates SAML assertions when configured as an identity provider.

Use the identity provider event log if your users have errors when trying to log in to your service provider's apps.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

Define and modify identity providers and service providers:

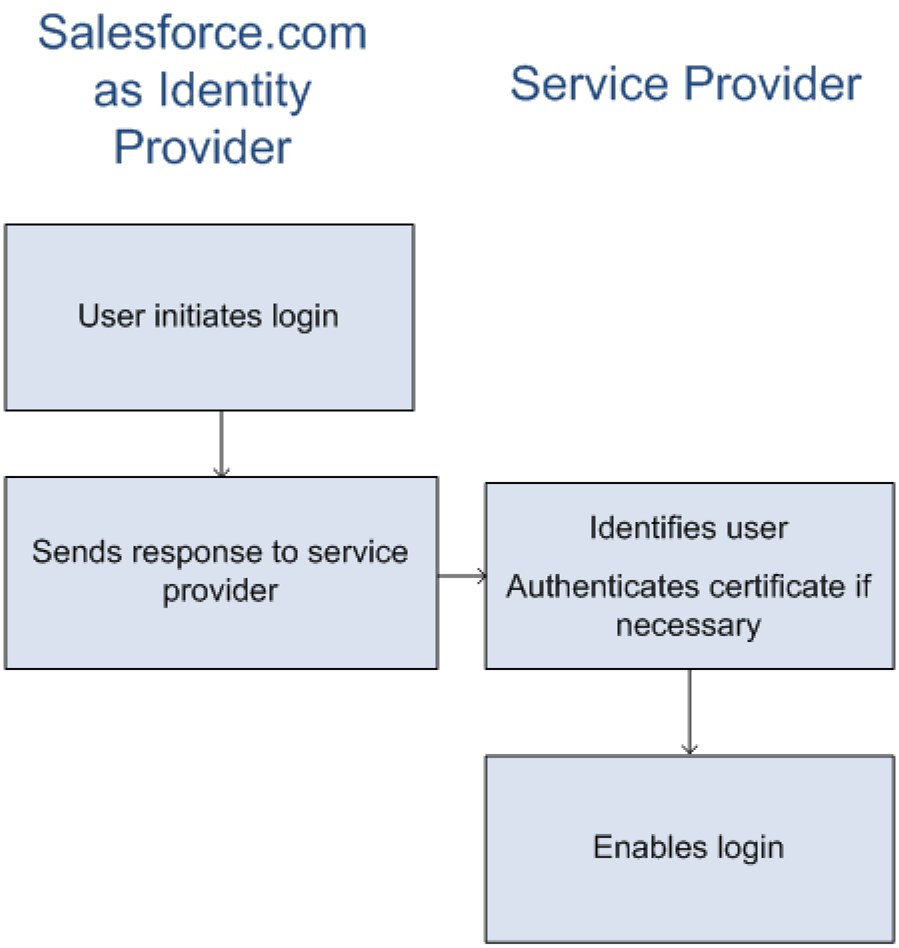
- Customize Application

Using Identity Providers and Service Providers

Salesforce supports the following:

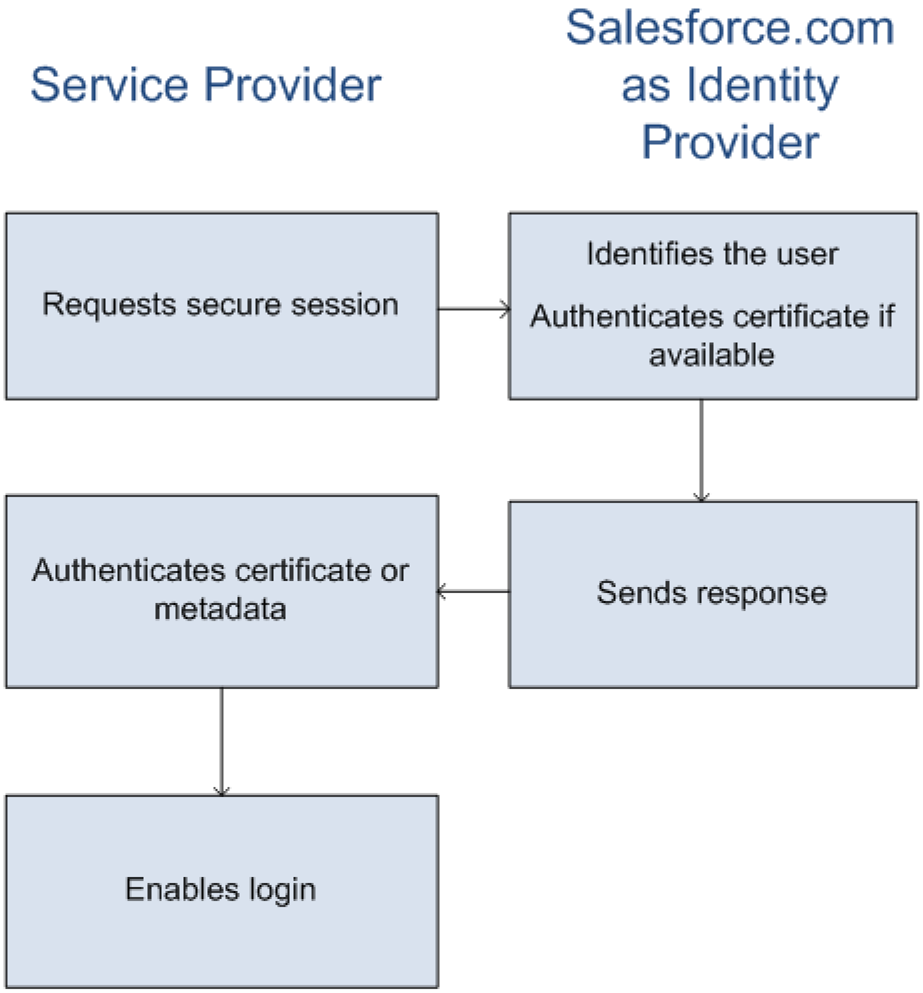
- Identity-provider-initiated login—when Salesforce logs in to a service provider at the initiation of the end user
- Service-provider-initiated login—when the service provider requests Salesforce to authenticate a user, at the initiation of the user

Here's the general flow when Salesforce is an identity provider and logs in to a service provider.


Salesforce.com as Identity Provider
Service Provider
User initiates login
Sends response to service provider
Identifies user
Authenticates certificate if necessary
Enables login

1. The user tries to access a service provider already defined in Salesforce.
2. Salesforce sends a SAML response to the service provider.
3. The service provider identifies the user and authenticates the certificate.
4. If the user is identified, the user's logged in to the service provider.

Here's the general flow when a service provider initiates the login process and uses Salesforce to identify the user.


Service Provider
Salesforce.com as Identity Provider
Requests secure session
Identifies the user
Authenticates certificate if available
Sends response
Authenticates certificate or metadata
Enables login

1. The service provider sends a valid SAML request. The SP-Initiated POST endpoint is generated when the service provider is defined.
2. Salesforce identifies the user specified in the SAML request.

```
<samlp:AuthnRequest ID="bndkmeemcaamihajeloilkagfdliilbhjjnmlmfo" Version="2.0"
   IssueInstant="2010-05-24T22:57:19Z"
   ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
   ProviderName="google.com" IsPassive="false"
   AssertionConsumerServiceURL="https://www.google.com/a/resp.info/acs">
   <saml:Issuer>google.com</saml:Issuer>
   <samlp:NameIDPolicy AllowCreate="true"
   Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>
</samlp:AuthnRequest>
```

If a certificate is part of the definition, Salesforce authenticates the certificate.

Note: If the service provider definition includes a certificate but the SAML request doesn't contain a certificate, the request fails and the user isn't logged in to Salesforce. If the definition doesn't include a certificate and the request includes a signature, the request succeeds if the user is identified correctly.

3. The user is prompted to log in to Salesforce if not logged yet.
4. Salesforce sends a SAML response to the service provider.

5. The service provider authenticates the SAML response sent by Salesforce. If the user is authenticated, the user is logged in to the service provider and logged in to Salesforce.

   Important: Salesforce doesn't provide a mechanism for logging users out of Salesforce when they log out of the service provider.

The following is an example of the SAML response from Salesforce. Share this information with your service provider.

```
<samlp:Response Destination="https://login-blitz03.soma.salesforce.com/
?saml=MgoTx78aEPa2r1BHKCHmlfUKhH2mkDrXOjmYcjHG_qNDbsRM_6ZAo.wvGk"
  ID="_0f551f9288c8b76f21c3d4d15c9cd1df1290476801091"
  InResponseTo="_2INwHuINDJTvjo8ohcM.Fpw_uLukYi0WArVx2IJD569kZYL
    osBwuiaSbzzxOPQjDtfw52tJB10VfgPW2p5g7Nlv5k1QDzR0EJYGgn0d0z8
    CIiUOY31YBdk7gwEkTygiK_lb46IO1fzBFoaRTzwvf1JN4qnkGttw3J6L4b
    opRI8hSQmCumM_Cvn3DHZVN.KtrzzOAflcMFSCY.bj1wvruSGQCooTRSSQ"
  IssueInstant="2010-11-23T01:46:41.091Z" Version="2.0">
<saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
>identityorg.blitz03.blitz.salesforce.com</saml:Issuer>
–
<ds:Signature>
–
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
–
<ds:Reference URI="#_0f551f9288c8b76f21c3d4d15c9cd1df1290476801091">
–
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
–
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<ec:InclusiveNamespaces PrefixList="ds saml samlp xs"/>
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>4NVTbQ2WavD+ZBiyQ7ufc8EhtZw=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
–
<ds:SignatureValue>

eqrkFxNlJRCT4VQ7tt7wKZGK7oLCCCa4gV/HNcL03RoKbSXIcwU2CAqW0qTSj25FqhRe2fOwAYa5
xFWat7Fw2bbncU+/nnuVNZut8HEEQoHiQA/Jrh7XB4CNlOpM1QRvgB5Dtdkj/0lI4h3X3TFix57B
sgZJGbb5PWEqSH3ZAl+NPvW9nNtYQIFyCTe9+cw2BhCxFgSWfP3/kIYHSM2gbIy27CrRrFS1lAqP
hKSLaH+ntH1E09gp78RSyJ2WKFGJU22sE9RJSZwdVw3VGG06Z6RpSjPJtaREELhhIBWTHNoF+VvJ
2Hbexjew6CO08lXRDe8dbrrPIRK/qzHZYf1H0g==
</ds:SignatureValue>
–
<ds:KeyInfo>
–
<ds:X509Data>
–
<ds:X509Certificate>
MIIEbjCCA1agAwIBAgIOASh04QulAAAAAClXs7MwDQYJKoZIhvcNAQEFBQAwfTEVMBMGA1UEAwwM
```

```
SWRlbnRpdHkgT3JnMRgwFgYDVQQLDA8wMEREMDAwMDAwMEZIOGwxFzAVBgNVBAoMDlNhbGVzZm9y
Y2UuY29tMRYwFAYDVQQHDA1TYW4gRnJhbmNpc2NvMQswCQYDVQQIDAJDQTEMMAoGA1UEBhMDVVNB
MB4XDTEwMDUwNzIyMjcwNVoXDTEyMDUwNjIyMjcwNVowfTEVMBMGA1UEAwwMSWRlbnRpdHkgT3Jn
MRgwFgYDVQQLDA8wMEREMDAwMDAwMEZIOGwxFzAVBgNVBAoMDlNhbGVzZm9yY2UuY29tMRYwFAYD
VQQHDA1TYW4gRnJhbmNpc2NvMQswCQYDVQQIDAJDQTEMMAoGA1UEBhMDVVNBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyM4/sjoaizbnWTDjt9mGht2fDGxnLCWGMJ+D+9NWXD5wM15N
SFEcflpI9W4makcCGvoac+CVbPTmOUzOsCQzu7iGkLeMMpngf2XqllnJgl4ejuH8socNrDtltaMk
hC08KAmli3Wm/okllqSjVOl8H52jtbvm6HkvLVj2NDLRY6kUejVZMGjGwV5E0FJliwgIip4sCchl
dkahbNjbikiiv1MAs8xHbtBt3wnKZWJq3JtS0va1sazUVmEwGDlVW43QPF0S7eV3IJFFhyCPV8yF
N3k0wCkCVBWoknwkMA8CbD+p6qNBVmvh3F3IaW2oym/1eSvtMLNtrPJeZzssqDYqgQIDAQABo4Hr
MIHoMB0GA1UdDgQWBBTYSVEZ9r8Q8T2rbZxPFfPYPZKWITCBtQYDVR0jBIGtMIGqgBTYSVEZ9r8Q
8T2rbZxPFfPYPZKWIaGBgaR/MH0xFTATBgNVBAMMDElkZW50aXR5IE9yZzEYMBYGA1UECwwPMDBE
RDAwMDAwMDBGSDhsMRcwFQYDVQQKDA5TYWxlc2ZvcmNlLmNvbTEWMBQGA1UEBwwNU2FuIEZyYW5j
aXNjbzELMAkGA1UECAwCQ0ExDDAKBgNVBAYTA1VTQYIOASh04QupAAAAAClXs7MwDwYDVR0TAQH/
BAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEANaO5Tqcc56E6Jv8itwjtbPvR+WHEMnZgQ9cCPF5Q
VACd5v7I/srx4ZJt/ZO4RZkmX1FXla0M7JGOu63eELHYG1DxT1SpGmpOL7xfBn7QUoh8Rmpp3BZC
WCPIcVQHLs1LushsrpbWu+85tgzlVN4sFVBl8F9rohhbM1dMOUAksoQgM3avcZ2vkugKhX40vIuf
Gw4wXZe4TBCfQay+eDONYhYnmlxVV+dJyHheENOYfVqlau8RMNhRNmhXlGxXNQyU3kpMaTxOux8F
DyOjc5YPoe6PYQ0C/mC77ipnjJAjwm+Gw+heK/9NQ7fIonDObbfu2rOmudtcKG74IDwkZL8HjA==
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
–
<samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>
–
<saml:Assertion ID="_e700bf9b25a5aebdb9495fe40332ef081290476801092"
IssueInstant="2010-11-23T01:46:41.092Z" Version="2.0">
<saml:Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">identityorg.blitz03.blitz.salesforce.com</saml:Issuer>
–
<saml:Subject>
<saml:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">charliemortimore@gmail.com</saml:NameID>
–
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData NotOnOrAfter="2010-11-23T01:51:41.093Z"
Recipient="https://login-blitz03.soma.salesforce.com/?saml=MgoTx78aEPa2r1BHKCHmlfUKhH2mkDrXOjmYcjHG_qNDbsRM_6ZAo.wvGk"/>
</saml:SubjectConfirmation>
</saml:Subject>
–
<saml:Conditions NotBefore="2010-11-23T01:46:41.093Z"
NotOnOrAfter="2010-11-23T01:51:41.093Z">
–
<saml:AudienceRestriction>
<saml:Audience>https://childorgb.blitz03.blitz.salesforce.com</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
–
<saml:AuthnStatement AuthnInstant="2010-11-23T01:46:41.092Z">
–
```

```
<saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:AuthnStatement>
–
<saml:AttributeStatement>
–
<saml:Attribute Name="userId"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xsi:type="xs:anyType">005D0000001Ayzh</saml:AttributeValue>
</saml:Attribute>
–
<saml:Attribute Name="username"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xsi:type="xs:anyType">admin@identity.org</saml:AttributeValue>
</saml:Attribute>
–
<saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xsi:type="xs:anyType">cmortimore@salesforce.com</saml:AttributeValue>
</saml:Attribute>
–
<saml:Attribute Name="is_portal_user"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xsi:type="xs:anyType">false</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
```

IN THIS SECTION:

Enable Salesforce as an Identity Provider

Salesforce can act as a single sign-on (SSO) identity provider to service providers, allowing end users to easily and securely access many web and mobile applications with one login. When using SAML for federated authentication, enable Salesforce as an identity provider and then set up connected apps. However, the OpenID Connect protocol for SSO authentication doesn't require enabling Salesforce as an identity provider.

View Your Identity Provider Details

Prerequisites for Defining Service Providers

Before you define a service provider in Salesforce, follow these steps to define an identity provider and exchange configuration information with your provider.

Defining Service Providers as SAML-Enabled Connected Apps

Map Salesforce Users to App Users

View Your Service Provider Details

Enabling Identity Providers and Defining Service Providers for Portals and Sites

Using the Identity Provider Event Log

Examples for Setting Up Identity Providers and Service Providers

SEE ALSO:

Enable Salesforce as an Identity Provider

View Your Identity Provider Details

Prerequisites for Defining Service Providers

Defining Service Providers as SAML-Enabled Connected Apps

Map Salesforce Users to App Users

View Your Service Provider Details

Enabling Identity Providers and Defining Service Providers for Portals and Sites

Examples for Setting Up Identity Providers and Service Providers

Enable Salesforce as an Identity Provider

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

Define and modify identity providers and service providers:

- Customize Application

Salesforce can act as a single sign-on (SSO) identity provider to service providers, allowing end users to easily and securely access many web and mobile applications with one login. When using SAML for federated authentication, enable Salesforce as an identity provider and then set up connected apps. However, the OpenID Connect protocol for SSO authentication doesn't require enabling Salesforce as an identity provider.

1. Configure a domain using My Domain and deploy it to all users. For instructions, see Set Up a My Domain Name.
2. From Setup, enter `Identity Provider` in the Quick Find box, select **Identity Provider**, and click **Enable Identity Provider**.
3. By default, a Salesforce identity provider uses a self-signed certificate generated with the SHA-256 signature algorithm. If you've already created self-signed certificates, select the certificate to use when securely communicating with other services.

   If you want to use a CA-signed certificate instead of self-signed certificate, follow these steps.

   a. Create and import a CA-signed certificate. For instructions, see Generate a Certificate Signed by a Certificate Authority.

   b. From Setup, enter `Identity Provider` in the Quick Find box, then select **Identity Provider**.

   c. Click **Edit**, and then select the CA-signed certificate.

   d. Click **Save**.

After you enable Salesforce as an identity provider, you can create connected apps to provide access to service providers.

SEE ALSO:

Identity Providers and Service Providers

Generate a Self-Signed Certificate

Create a Connected App

View Your Identity Provider Details

After you enable an identity provider for your organization, you can view the details from Setup by entering *Identity Provider* in the Quick Find box, then selecting **Identity Provider**. You might need to share this information, such as Issuer, with your service provider.

From this page you can click:

- **Edit** to change the certificate associated with your identity provider.

  Warning: Changing the certificate can disable access to external applications. You might need to update all external applications to validate the new certificate information.

- **Disable** to disable your identity provider.

  Warning: If you disable your identity provider, users can no longer access any external applications.

- **Download Certificate** to download the certificate associated with your identity provider. Your service provider can use this information for connecting to Salesforce.
- **Download Metadata** to download the metadata associated with your identity provider. Your service provider can use this information for connecting to Salesforce.
- In the SAML Metadata Discovery Endpoints section, you can access URLs for the SAML identity provider information for your custom domain and each community. Your service provider can use these URLs to configure single sign-on to connect to Salesforce.
  - Salesforce Identity—URL of identity provider metadata for your custom domain in My Domain.
  - *Community Name* Community Identity—URL of identity provider metadata for the named community.
- In the service providers section, next to the name of an existing service provider, click **Edit** to change its definition, click **Profiles** to add or remove user profiles that have access to this service provider, or click **Del** to delete it.

  Note: To define a new service provider, from Setup, enter *Apps* in the Quick Find box, then select **Apps** and then create a new SAML-enabled connected app.

SEE ALSO:

Identity Providers and Service Providers

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

Define and modify identity providers and service providers:

- Customize Application

Prerequisites for Defining Service Providers

Before you define a service provider in Salesforce, follow these steps to define an identity provider and exchange configuration information with your provider.

1. Enable Salesforce as an identity provider.
2. Give your service provider information about your configuration of Salesforce as an identity provider. This information is available as metadata that you can download and give to your service provider. To obtain this metadata, from Setup, enter `Identity Provider` in the `Quick Find` box, select **Identity Provider**, then click **Download Metadata**.

   If your service provider doesn't support metadata, but supports certificates instead, you can download the certificate. From Setup, enter `Identity Provider` in the `Quick Find` box, then select **Identity Provider**, then click **Download Certificate**.
3. Get the following information from your service provider:
   - Assertion consumer service (ACS) URL
   - Entity ID
   - Subject type—Specifies if the subject for the SAML response from Salesforce (as an identity provider) is a Salesforce user name or a federation ID
   - Security certificate—Only required when the service provider is initiating login to Salesforce and signing their SAML requests

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

Define and modify identity providers and service providers:
- Customize Application

SEE ALSO:

Identity Providers and Service Providers

Defining Service Providers as SAML-Enabled Connected Apps

1. Complete the prerequisites.
2. From Setup, enter `Apps` in the `Quick Find` box, then select **Apps**.
3. Under Connected Apps, click **New**.
4. Specify the required fields under Basic Information.
5. Under Web App Settings, select **Enable SAML** and then provide the following:

   Entity Id

   This value comes from the service provider. Each entity ID in an organization must be unique. If you're accessing multiple apps from your service provider, you only need to define the service provider once, and then use the `RelayState` parameter to append the URL values to direct the user to the correct app after signing in.

   ACS URL

   The ACS, or assertion consumer service, URL comes from the SAML service provider.

   Subject Type

   Specifies which field defines the user's identity for the app. Options include the user's username, federation ID, user ID, a custom attribute, or an algorithmically calculated persistent ID. A custom attribute can be any custom field added to the User object in the organization, as long as it is one of the following data types: Email, Text, URL, or Formula (with Text Return Type). After you select `Custom Attribute` for the **Subject Type**, Salesforce displays a **Custom Attribute** field with a list of the available User object custom fields in the organization.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

Define and modify identity providers and service providers:
- Customize Application

Name ID Format

Specifies the format attribute sent in SAML messages. “Unspecified” is selected by default. Depending on your SAML service provider, you may want to set this to email address, persistent, or transient.

Issuer

By default, the standard issuer for your identity provider is used (your organization’s My Domain). If your SAML service provider requires a different value, specify it here.

6. Optionally specify the following:

Start URL

Directs users to a specific location when they run the application. The Start URL can be an absolute URL, such as `https://na1.salesforce.com/001/o`, or it can be the link for the application name, such as `https://customer.goodApp.com` for GoodApp. Specifying a Start URL makes the application available in the Force.com app menu and in App Launcher.

Verify Request Signatures

Select `Verify Request Signatures` if the service provider gave you a security certificate. Browse your system for the certificate. This is only necessary if you plan to initiate logging in to Salesforce from the service provider and the service provider signs their SAML requests.

Important: If you upload a certificate, all SAML requests must be signed. If no certificate is uploaded, all SAML requests are accepted.

Encrypt SAML Response

Select `Encrypt SAML Response` to upload a certificate and select an encryption method for encrypting the assertion. Valid encryption algorithm values are `AES–128` (128–bit key). `AES–256` (256–bit key). and `Triple-DES` (Triple Data Encryption Algorithm).

7. Click **Save**.

To authorize users for this SAML application:

1. From Setup, enter *`Connected Apps`* in the `Quick Find` box, then select the option for managing connected apps.
2. Click the name of the application.
3. Select the profiles and/or permission sets that can access the application.

SEE ALSO:

Identity Providers and Service Providers

Custom Fields

Map Salesforce Users to App Users

If the `Subject Type` for the service provider definition is `Federation ID`, you must map the Salesforce user to the username used to sign into the service provider.

To map a Salesforce user to the app user:

1. From Setup, enter *`Users`* in the `Quick Find` box, then select **Users**, then click **Edit** for every user who needs to be mapped.
2. In `Federation ID`, under Single Sign On Information, enter the username to be used to log into the service provider.
3. Click **Save**.

Tip: Use SOAP API if you have a large number of user profiles or permission sets to update. See the *SOAP API Developer's Guide*.

SEE ALSO:

Identity Providers and Service Providers

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

Define and modify identity providers and service providers:
- Customize Application

View Your Service Provider Details

After you define a service provider for your organization by creating a SAML-enabled connected app, you can view the details from Setup by entering *`Connected Apps`* in the `Quick Find` box, then selecting **Connected Apps**, and then selecting the name of the app. You might need to share this information, such as `SP-Initiated POST Endpoint` or `SP-Initiated Redirect Endpoint`, with your service providers.

From this page you can click:

- **Edit** to change the values of the service provider definition.
- **Delete** to delete a service provider definition.

  Warning: If you delete a service provider definition, your users will no longer have access to that service provider.

- **Profile Access** to change which profiles have access to this service provider.

SEE ALSO:

Identity Providers and Service Providers

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

Define and modify identity providers and service providers:
- Customize Application

Enabling Identity Providers and Defining Service Providers for Portals and Sites

When enabling identity providers and defining service providers for Force.com Sites, Customer Portals and partner portals, note the following:

- When defining a service provider, if the `Subject Type` is `Username`, the Salesforce organization ID is prepended to the user name in the SAML assertion. For example, if the user is `jDeoint@WFC.com`, the subject for the SAML assertion contains `00DE0000000FFLT@jDeoint@WFC.com`. If the `Subject Type` is `Federation ID`, the exact federation ID is used.
- The attribute `is_portal_user` included in the SAML assertion generated by Salesforce contains values. You might want to share the following example with your service provider.

```
<saml:Attribute Name="is_portal_user"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue
         xmlns:xs="http://www.w3.org/2001/XMLSchema"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:type="xs:anyType">true
      </saml:AttributeValue>
</saml:Attribute>
```

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

Define and modify identity providers and service providers:

- Customize Application

SEE ALSO:

Identity Providers and Service Providers

Using the Identity Provider Event Log

The identity provider event log records both problems and successes with inbound SAML authentication requests from another app provider, and outbound SAML responses when Salesforce is acting as an identity provider. To view the identity provider event log, from Setup, enter `Identity Provider Event Log` in the `Quick Find` box, then select **Identity Provider Event Log**. You can show successes, failures, or both in the log. You can view the 50 most recent events in the UI; you can view more by creating a report.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

Define and modify identity providers and service providers:

- Customize Application

Examples for Setting Up Identity Providers and Service Providers

These examples show you how to set up Salesforce as an identity provider with different connected apps. End users can then authenticate to Salesforce and access other service providers using single sign-on (SSO).

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Tabs are not available in **Database.com**

USER PERMISSIONS

Define and modify identity providers and service providers:

- Customize Application

IN THIS SECTION:

Configure Salesforce as an Identity Provider for Amazon Web Services Authentication

Let your users log in to Amazon Web Services (AWS) using their Salesforce credentials and a connected app.

Configure Salesforce as an Identity Provider for Google Apps Authentication

Let your users log in to Google Apps using their Salesforce credentials and a connected app.

Configure Salesforce as an Identity Provider for Office 365 Authentication

Let your users log in to Office 365 using their Salesforce credentials and a connected app.

Configure SSO to Salesforce Using Microsoft Active Directory Federation Services as the Identity Provider

Let your users log in from a Microsoft environment to a Salesforce org using Microsoft Active Directory Federation Services (AD FS) 2.0. Microsoft AD FS functions as the identity provider for single sign-on authentication.

SEE ALSO:

Identity Providers and Service Providers

Personalize Your Salesforce Experience

Configure Salesforce as an Identity Provider for Amazon Web Services Authentication

Let your users log in to Amazon Web Services (AWS) using their Salesforce credentials and a connected app.

Configuring Salesforce as an identity provider for AWS involves these high-level steps.

1. On Salesforce, configure a subdomain with My Domain and get a certificate.
2. On AWS, supply the required information from your Salesforce configuration.
3. On Salesforce, create a connected app to run AWS in Salesforce.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

Enable and Deploy My Domain on Your Salesforce Org

If you haven't already done so, use Salesforce My Domain to create your own subdomain under my.salesforce.com. Enabling My Domain creates a Salesforce Identity Provider (IdP). Use the My Domain wizard to set up a subdomain.

1. From Setup, enter `My Domain` in the Quick Find box, and then select **My Domain**.
2. Deploy the subdomain to your users.

Warning: Deploying a domain on existing orgs can impact user bookmarks. Make sure that your users are aware of this possibility before you deploy the subdomain on existing production orgs.

Get a SAML IdP Certificate

Get a certificate, either self-signed or issued by a certificate authority, to use to set up service providers. Save the certificate on your local drive.

Download the Metadata Document

1. From Setup, enter `Identity` in the Quick Find box, and then select **Identity Provider**.
2. Click **Download Metadata**.

On the same page under SAML Metadata Discovery Endpoints, make note of the Salesforce Identity, for example, https://yourdomain.my.salesforce.com/.well-known/samlidp.xml. The identity begins with the name of your subdomain.

Create a SAML Provider on AWS

Follow AWS instructions to create a SAML identity provider. Log in to the AWS Console as an administrator, navigate to Identity Providers, and follow the instructions to create a SAML provider. AWS generates an Amazon resource number (ARN) for the provider, which you need in a later step.

1. Upload the metadata document from your local drive. AWS generates the ARN for your identity provider, for example, arn:aws:iam::365652557137:saml-provider/salesforce. Save the ARN to your local drive.
2. Create one or more roles with the desired policy for users. For each role:
   a. Create a role for Identity Provider Access.
   b. Grant Web Single-Sign-On (WebSSO) access to SAML providers.
   c. Set the desired permissions.
   d. Save the ARN for the role, for example, arn:aws:iam::365652557137:role/SSOUserRole.

Create and Configure a Connected App on Salesforce

1. Use the New Connected App wizard to define a connected app.
    - In Lightning Experience, you use the App Manager to create connected apps. From Setup, enter `App` in the Quick Find box, then select **App Manager**. Click **New Connected App**.
    - In Salesforce Classic, from Setup, enter `Apps` in the Quick Find box, then select **Apps**. On that page under Connected Apps, click **New**.

2. Configure settings for the connected app.

    Under Basic Information:

    a. Name the app Amazon Web Services.

    b. Enter your own email address.

    Under Web App Settings:

    a. Select **Enable SAML**.

    b. For Entity Id, enter `https://signin.aws.amazon.com/saml`.

    c. For ACS URL, enter `https://signin.aws.amazon.com/saml`.

    d. For Subject Type, select **Persistent ID**.

    e. For Name ID Format, select **urn:oasis:names:tc:SAML:2.0:nameid-format:persistent**.

    f. For Issuer, keep the default value, your subdomain.

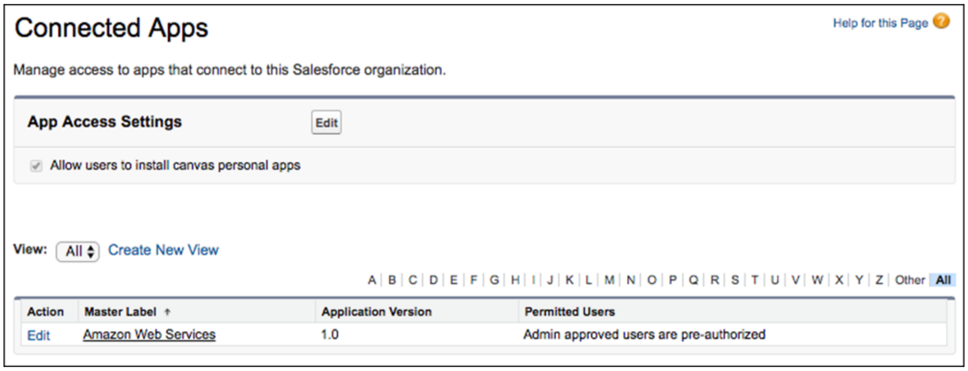
    g. In the field IdP Provider Certificate, keep the default (unselected).

    h. For Verify Request Signatures, keep the default (unselected).

    i. Click **Save**.

    Note: It can take a few minutes for Salesforce to create the connected app.

3. From Setup, enter `Apps`, in the Quick Find box. If you're using Lightning Experience, select **Manage Connected Apps**. If you're using Salesforce Classic, under **Manage Apps** select **Connected Apps** .



Connected Apps

Manage access to apps that connect to this Salesforce organization.

App Access Settings

☑ Allow users to install canvas personal apps

View: All Create New View

Action	Master Label ↑	Application Version	Permitted Users
Edit	Amazon Web Services	1.0	Admin approved users are pre-authorized

Help for this Page
Edit
A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | Other | All

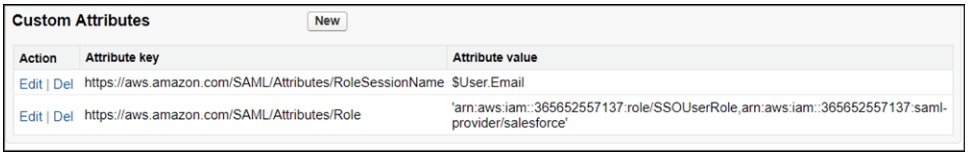
4. Click **Amazon Web Services**. The connected app detail page appears.

5. Under Custom Attributes, click **New** to create custom attributes.

    a. For the attribute key, enter `https://aws.amazon.com/SAML/Attributes/RoleSessionName`. For the attribute value, enter `$User.Email`.

b. For the next attribute key, enter `https://aws.amazon.com/SAML/Attributes/Role`. For the attribute value, enter `'arn:aws:iam::365652557137:role/SSOUserRole,arn:aws:iam::365652557137:saml-provider/salesforce'`.

The attribute value is the saved AWS ARN value for the role and the ARN value for the IdP provider, separated by a comma and entered within single quotes.



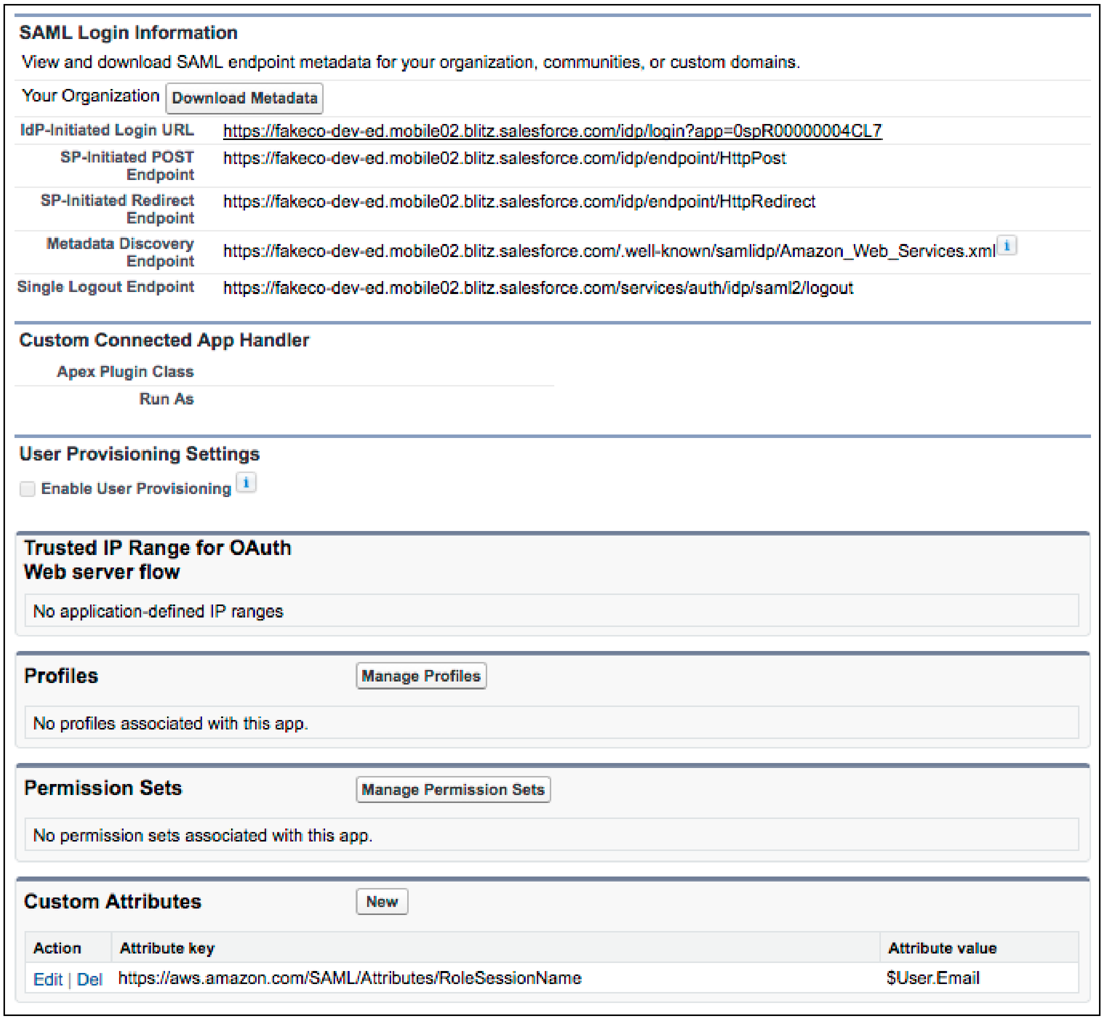
Custom Attributes

Action	Attribute key	Attribute value
Edit | Del	https://aws.amazon.com/SAML/Attributes/RoleSessionName	$User.Email
Edit | Del	https://aws.amazon.com/SAML/Attributes/Role	'arn:aws:iam::365652557137:role/SSOUserRole,arn:aws:iam::365652557137:saml-provider/salesforce'

Tip: Consider creating a custom user attribute as a picklist with your Amazon roles, allowing you to dynamically select a user's role.

6. Configure the Start URL for the connected app.

a. On the connected app detail page, copy the IdP-Initiated Login URL from under SAML Login Information.



SAML Login Information

View and download SAML endpoint metadata for your organization, communities, or custom domains.

Your Organization	Download Metadata
IdP-Initiated Login URL	https://fakeco-dev-ed.mobile02.blitz.salesforce.com/idp/login?app=0spR00000004CL7
SP-Initiated POST Endpoint	https://fakeco-dev-ed.mobile02.blitz.salesforce.com/idp/endpoint/HttpPost
SP-Initiated Redirect Endpoint	https://fakeco-dev-ed.mobile02.blitz.salesforce.com/idp/endpoint/HttpRedirect
Metadata Discovery Endpoint	https://fakeco-dev-ed.mobile02.blitz.salesforce.com/.well-known/samlidp/Amazon_Web_Services.xml
Single Logout Endpoint	https://fakeco-dev-ed.mobile02.blitz.salesforce.com/services/auth/idp/saml2/logout

Custom Connected App Handler

Apex Plugin Class

Run As

User Provisioning Settings

□ Enable User Provisioning

Trusted IP Range for OAuth Web server flow

No application-defined IP ranges

Profiles

No profiles associated with this app.

Permission Sets

No permission sets associated with this app.

Custom Attributes

Action	Attribute key	Attribute value
Edit | Del	https://aws.amazon.com/SAML/Attributes/RoleSessionName	$User.Email

b. Click **Edit Policies**.

c. For Start URL under Basic Information, paste the IdP-Initiated Login URL and click **Save**.

7. Under Profiles or Permission Sets, add the profiles or permission sets of users who can access this app.
8. To test access, run the connected app as an end user.

SEE ALSO:

Connected Apps

Create a Connected App

Configure Salesforce as an Identity Provider for Google Apps Authentication

Let your users log in to Google Apps using their Salesforce credentials and a connected app.

Configuring Salesforce as an identity provider for Google Apps involves these high-level steps.

1. On Salesforce, configure a subdomain with My Domain and get a certificate.
2. On Google Apps, supply the required information from your Salesforce configuration.
3. On Salesforce, create a connected app to run Google Apps in Salesforce.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

Enable and Deploy My Domain on Your Salesforce Org

If you haven't already done so, use Salesforce My Domain to create your own subdomain under my.salesforce.com. Enabling My Domain creates a Salesforce Identity Provider (IdP). Use the My Domain wizard to set up a subdomain. For more information, see Set Up a My Domain Name.

1. From Setup, enter `My Domain` in the Quick Find box, and then select **My Domain**.
2. Deploy the subdomain to your users.

Warning: Deploying a domain on existing orgs can impact user bookmarks. Make sure that your users are aware of this possibility before you deploy the subdomain on existing production orgs.

Get a SAML IdP Certificate

Get a certificate, either self-signed or issued by a certificate authority, to use to set up service providers.

Download the Metadata Document

1. From Setup, enter `Identity` in the Quick Find box, and then select **Identity Provider**.
2. Click **Download Metadata**.

On the same page under SAML Metadata Discovery Endpoints, make note of the Salesforce Identity, for example, https://yourdomain.my.salesforce.com/.well-known/samlidp.xml. The identity begins with the name of your subdomain.

Configure a SAML Provider in Google Apps

1. Sign in as an administrator to the Google Apps account using `https://admin.google.com`.
2. Navigate to the Google Apps page for configuring single sign-on.
3. For the sign-in page URL, enter `https://yourdomain.my.salesforce.com/idp/endpoint/HttpRedirect`, replacing `yourdomain` with your My Domain.
4. For the sign-out page URL, enter `https://yourdomain.my.salesforce.com/`, replacing `yourdomain` with your My Domain.

5. For the change password URL, enter `https://yourdomain.my.salesforce.com/_ui/system/security/ChangePassword`, replacing `yourdomain` with your My Domain.
6. For the verification certificate, upload the SAML IdP certificate you obtained earlier.
7. Select **Use a domain specific issuer**.
8. Click **Save changes**.

Create and Configure a Connected App on Salesforce

1. Define a connected app.
   - In Lightning Experience, from Setup, enter *App* in the Quick Find box, and select **App Manager**. Click **New Connected App**.
   - In Salesforce Classic, from Setup, enter *Apps* in the Quick Find box, and select **Apps**. Under Connected Apps, click **New**.

2. Configure the connected app.

   Under Basic Information:

   a. Name the app (for example, Gmail).

   b. Enter your own email address.

   Under Web App Settings:

   a. Select **Enable SAML**.

   b. For Entity Id, enter `https://google.com`.

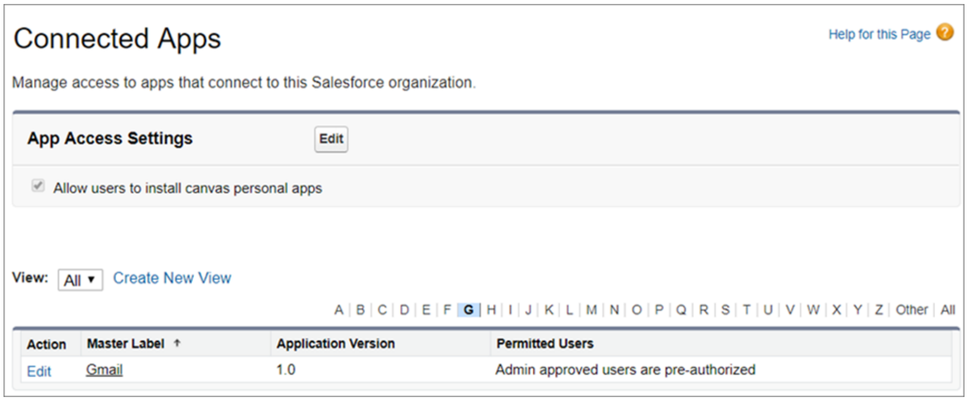
   c. For ACS URL, enter the URL for your Google App account.

   d. For Subject Type, set the method attribute by which a user name in Google Apps maps to a unique Salesforce user identity. For example, to use federated authentication, select **Federation ID**. For more information, see Best Practices for Implementing Single Sign-On.

   e. Click **Save**.

   Note: It can take a few minutes for Salesforce to create the connected app.

3. From Setup, enter *Apps*, in the Quick Find box. If you're using Lightning Experience, select **Manage Connected Apps**. If you're using Salesforce Classic, under Manage Apps select **Connected Apps**.


Help for this Page
Edit
View: All ▾ Create New View
A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | Other | All

Connected Apps

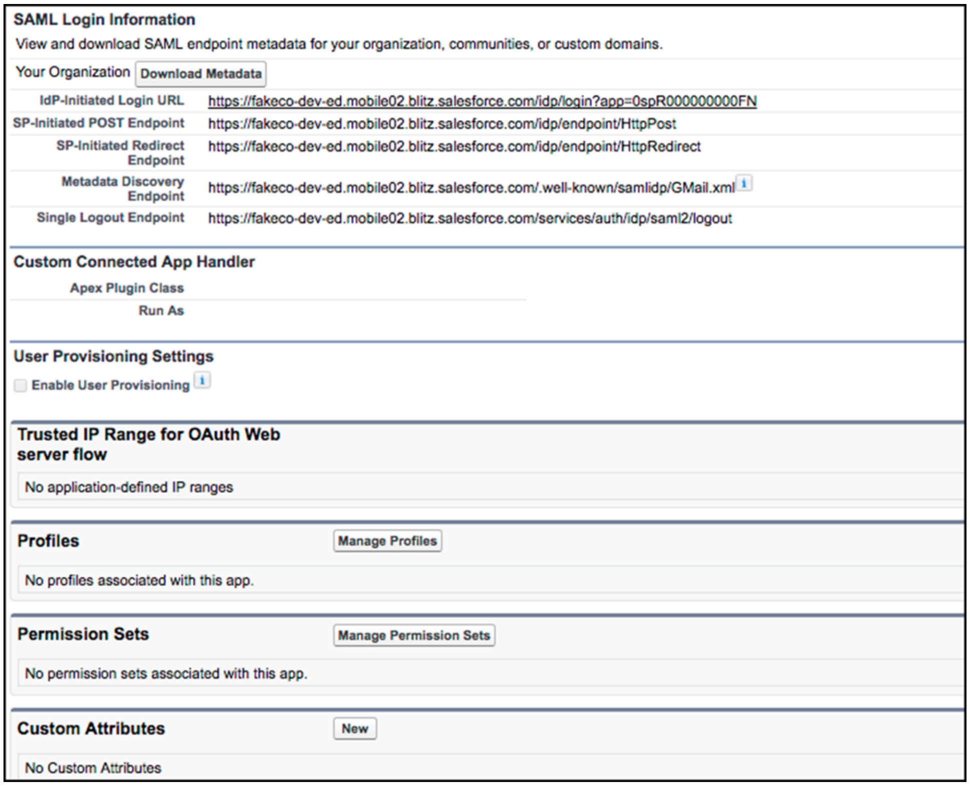
Manage access to apps that connect to this Salesforce organization.

App Access Settings

☑ Allow users to install canvas personal apps

Action	Master Label ↑	Application Version	Permitted Users
Edit	Gmail	1.0	Admin approved users are pre-authorized

4. Click **Gmail**.
5. Under SAML Login Information, copy the IdP-initiated login URL.



SAML Login Information

View and download SAML endpoint metadata for your organization, communities, or custom domains.

Your Organization Download Metadata

IdP-Initiated Login URL	https://fakeco-dev-ed.mobile02.blitz.salesforce.com/idp/login?app=0spR000000000FN
SP-Initiated POST Endpoint	https://fakeco-dev-ed.mobile02.blitz.salesforce.com/idp/endpoint/HttpPost
SP-Initiated Redirect Endpoint	https://fakeco-dev-ed.mobile02.blitz.salesforce.com/idp/endpoint/HttpRedirect
Metadata Discovery Endpoint	https://fakeco-dev-ed.mobile02.blitz.salesforce.com/.well-known/samlidp/GMail.xml
Single Logout Endpoint	https://fakeco-dev-ed.mobile02.blitz.salesforce.com/services/auth/idp/saml2/logout

Custom Connected App Handler

Apex Plugin Class

Run As

User Provisioning Settings

□ Enable User Provisioning

Trusted IP Range for OAuth Web server flow

No application-defined IP ranges

Profiles Manage Profiles

No profiles associated with this app.

Permission Sets Manage Permission Sets

No permission sets associated with this app.

Custom Attributes New

No Custom Attributes

a. Click **Edit Policies**.

b. For Start URL under Basic Information, paste the IdP-initiated login URL, and then click **Save**.

6. Under Profiles or Permission Sets, add the profiles or permission sets of users who can access this app.

Test the Connected App

Verify that your Salesforce org can use SSO to access the connected app.

1. Log out of Google Apps and Salesforce.
2. Try to access a Google App page, such as *`http://mail.google.com/a/respond.info/`*.
3. You are redirected to a Salesforce sign-on page. After you log in, you are at the specified Google App page.

An alternate test is to add the Google App to a web tab in your Salesforce org.

1. Log in to Salesforce.
2. From Setup, enter *`Tabs`* in the Quick Find box, select **Tabs**.
3. Under Web Tabs, click **New**.
4. Choose a tab layout, and click **Next**.
5. Enter a label for the tab. Use the default name, which is the same as the label.
6. To display the Tab Style Selector, click the **Tab Style** lookup icon. Select an icon. Keep all other defaults.
7. Click **Next**.
8. For Button or Link URL, enter a Google App page, such as *`mail.google.com/a/respond.info/`* for Gmail, and click **Next**.

   Note: Enter an absolute URL that contains either http:// or https://.

9. Click **Next** and then click **Save**.
10. To test the configuration, click the new tab at the top of your page. You are automatically logged in to the Google App page.

SEE ALSO:

Connected Apps

Create a Connected App

Configure Salesforce as an Identity Provider for Office 365 Authentication

Let your users log in to Office 365 using their Salesforce credentials and a connected app.

Configuring Salesforce as an identity provider for Office 365 involves these high-level steps.

1. On Salesforce, set up a subdomain with My Domain and obtain an SSL certificate.
2. On Office 365, configure Salesforce identity information for the domain.
3. On Salesforce, create and configure a connected app to run Office 365 in Salesforce.

You need the following to complete the steps.

- Admin account for Office 365
- Windows PowerShell for Azure Active Directory

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

Enable and Deploy My Domain on Your Salesforce Org

If you haven’t already done so, use Salesforce My Domain to create your own subdomain under my.salesforce.com. Enabling My Domain creates a Salesforce Identity Provider (IdP). Use the My Domain wizard to set up a subdomain.

1. From Setup, enter `My Domain` in the Quick Find box, and then select **My Domain**.
2. Deploy the subdomain to your users.

Warning: Deploying a domain on an existing org can impact user bookmarks. Make sure that your end users are aware of this behavior before you deploy the subdomain on existing production orgs.

Get a SAML IdP Certificate

Get a certificate, either self-signed or issued by a certificate authority, to use to set up service providers. Save the certificate on your local drive.

Download the Metadata Document

1. From Setup, enter `Identity` in the Quick Find box, and then select **Identity Provider**.
2. Click **Download Metadata**.

On the same page under SAML Metadata Discovery Endpoints, note the Salesforce Identity, for example, https://yourdomain.my.salesforce.com/.well-known/samlidp.xml. The identity begins with the name of your subdomain.

Configure Salesforce Identity Information for the Domain

1. Start the Windows Azure Active Directory module of Windows PowerShell.

2. Run the **$cred=Get-Credential** cmdlet, and provide the Windows Azure AD credentials of your Admin account.

```
PS C:\Windows\system32> $cred=Get-Credential
Cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
```

3. Run the **Connect-MsolService –Credential $cred** cmdlet.

```
PS C:\Windows\system32> Connect-MsolService –Credential $cred
```

4. Provide the required parameter values.

   - Your domain, for example, $dom = salesidentity.info
   - POST endpoint URL of the Salesforce IdP, for example, $url = https://yourdomainname.my.salesforce.com/idp/endpoint/HttpPost
   - IdP issuer, for example, $uri = https://yourdomainname.my.salesforce.com
   - IdP logout URL, for example, $logouturl = https://login.salesforce.com
   - IdP certificate, for example, $cert = <your certificate content>

   Note: Enter the certificate on a single line without line breaks.

```
PS C:\Windows\system32> $dom = salesidentity.info
PS C:\Windows\system32> $url =
https://yourdomainname.my.salesforce.com/idp/endpoint/HttpPost
PS C:\Windows\system32> $uri = https://yourdomainname.my.salesforce.com
PS C:\Windows\system32> $logouturl = https://login.salesforce.com
PS C:\Windows\system32> $cert = <your certificate content>
```

5. Run the **Set-MsolDomainAuthentication –DomainName $dom -FederationBrandName $dom -Authentication Federated -PassiveLogOnUri $url -SigningCertificate $cert -IssuerUri $uri -LogOffUri $logouturl -PreferredAuthenticationProtocol SAMLP** cmdlet to establish trust.

```
PS C:\Windows\system32> Set-MsolDomainAuthentication
–DomainName $dom -FederationBrandName $dom -Authentication
Federated -PassiveLogOnUri $url -SigningCertificate $cert
-IssuerUri $uri -LogOffUri $logouturl
-PreferredAuthenticationProtocol SAMLP
```

6. Run the **Get-MsolDomain** cmdlet to check whether Federation is Get enabled.

```
Name       Status Authentication
----       ------ --------------
salesforceidentity.info   Verified Federated
sfidentity.mail.onmicrosoft.com  Verified Managed
sfidentity.onmicrosoft.com   Verified Managed
```

7. Run the **Get-MsolDomainFederationSettings** cmdlet to verify the configuration.

Create and Configure a Connected App on Salesforce

1. From Setup, enter `Apps` in the Quick Find box. If you're using Lightning Experience, select **Manage Connected Apps**. If you're using Salesforce Classic, under Manage Apps, select **Connected Apps**.
2. Configure the connected app.

Under Basic Information:

a. Name the app `Office 365`.

b. Enter your own email address.

Under Web App Settings:

a. For Start URL, enter a URL and include a URL for your domain name.

```
https://login.microsoftonline.com/PostToIDP.srf?msg=AuthnReq&realm=
yourdomainname&wa=wsignin1.0&wtrealm=urn:federation:MicrosoftOnline&
wctx=bk%3D1367916313%26LoginOptions%3D3
```

b. Select **Enable SAML**.

c. For Entity Id, enter `urn:federation:MicrosoftOnline`.

d. For ACS URL, enter `https://login.microsoftonline.com/login.srf`.

e. For Subject Type, select **FederationID** or **Custom** attribute.

> Note: The subject type carries the ObjectGUID of UPN.

f. For Name ID Format, keep the default selection (unspecified).

g. For Issuer, keep the default value (your subdomain).

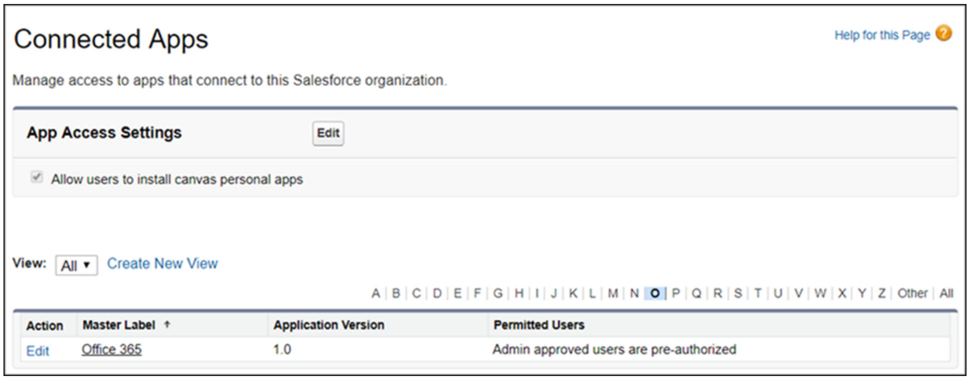
h. For Verify Request Signatures, keep the default (unselected).

i. For IdP Provider Certificate, keep the default (unselected).

j. Click **Save**.

> Note: It can take a few minutes for Salesforce to create the connected app.

3. From Setup, enter `Apps` in the Quick Find box. If you're using Lightning Experience, select **Manage Connected Apps**. If you're using Salesforce Classic, under Manage Apps, select **Connected Apps**.



Connected Apps

Manage access to apps that connect to this Salesforce organization.

App Access Settings

☑ Allow users to install canvas personal apps

View: All ▾ Create New View

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | Other | All

Action	Master Label ↑	Application Version	Permitted Users
Edit	Office 365	1.0	Admin approved users are pre-authorized

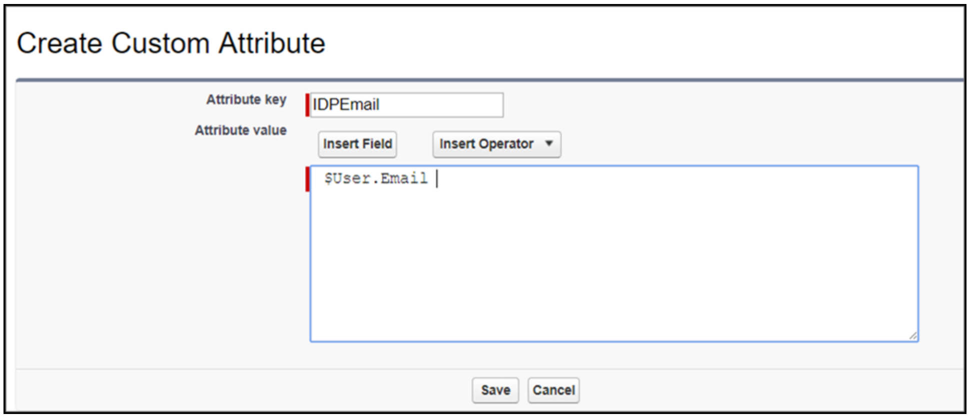
4. Select the **Office 365** connected app.

5. Click **Manage Profiles** or **Manage Permission Sets**, and add profiles and permission sets of users who can access this app.

6. Under **Custom Attributes**, click **New**.

a. Enter `IDPEmail` for the attribute key and `$User.Email` for the attribute value.

b. Click **Save**.



Create Custom Attribute

Attribute key: IDPEmail

Attribute value:

```
$User.Email
```

7. To test access, run the connected app as a user.

SEE ALSO:

Connected Apps

Create a Connected App

Configure SSO to Salesforce Using Microsoft Active Directory Federation Services as the Identity Provider

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

Let your users log in from a Microsoft environment to a Salesforce org using Microsoft Active Directory Federation Services (AD FS) 2.0. Microsoft AD FS functions as the identity provider for single sign-on authentication.

Microsoft AD FS 2.0 supports the SAML 2.0 protocol. When AD FS 2.0 is set up as a Salesforce identity provider, users can log in to Salesforce using single sign-on (SSO).

Note: When configuring AD FS 2.0 for use with Salesforce, it's recommended that you select **HTTP Redirect** in the Salesforce Single Sign-On settings under Service Provider Initiated Request Binding. This setting improves interoperability with iOS-based devices.

Prerequisites

To configure AD FS 2.0 as a Salesforce identity provider, you need:

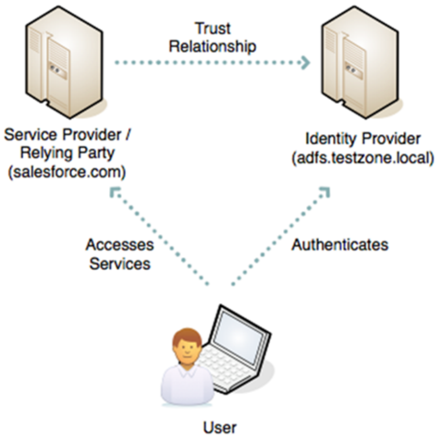
- Microsoft Windows Server 2008 R2 Enterprise or Datacenter edition. If you are configuring an environment for an evaluation, you can download a trial version from the Microsoft Download Center.
- Microsoft Active Directory Federation Services 2.0.

  Note: Windows Server 2008 R2 includes AD FS 1.0, which does not support SAML 2.0. For this reason, download the AD FS 2.0 'release to web' (RTW) package.

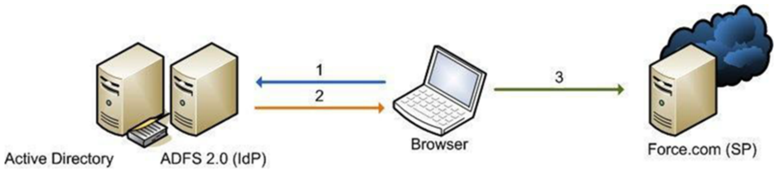
- A Salesforce org. If you're testing, a free Developer Edition environment is a great choice.

Overview

SAML 2.0 defines roles for parties involved in SSO. A user authenticates to the identity provider (IdP), in this case, AD FS 2.0. The user is then able to access a resource at one or more service providers (SP) without logging in at each service provider. The SP (also known as a "relying party") is in this instance a Salesforce org.


Trust Relationship
Service Provider / Relying Party (salesforce.com)
Identity Provider (adfs.testzone.local)
Accesses Services
Authenticates
User

Let’s first look at an overview of the process and then the configuration steps. This diagram shows the process for an IdP-initiated login into Salesforce. (Later on, we’ll look at SP-initiated login.)



1. The user authenticates to the AD FS server using Integrated Windows Authentication (Kerberos tokens over HTTP) and requests login to Salesforce.
2. AD FS returns a SAML assertion to the user’s browser.
3. The browser submits the assertion to Salesforce, which logs the user in.

Here are the high-level steps to create a test deployment.

- Install Microsoft AD FS 2.0
- Configure AD FS and your Salesforce environment
- Test the configuration
- Troubleshoot implementation problems as necessary

Install Software

1. Start by installing Windows Server 2008 R2.

   Note: The AD FS server must be a member of an Active Directory domain. If you’re building a lab setup for evaluation, the AD FS server can be the domain controller. However, this configuration is not a recommended production configuration.

2. Create a friendly DNS name for AD FS, such as adfs.testzone.local, and point it to your AD FS 2.0 server.
3. Download and install AD FS 2.0. This step installs other prerequisite Windows components, such as IIS.
4. In the IIS manager, create an SSL certificate for your friendly DNS name. If you have the IIS 6.0 resource kit, you can use SelfSSL to create a self-signed certificate.
5. Run through the AD FS Server configuration wizard.
   a. Create a federation service.
   b. Select **Stand-alone Server**.
   c. Select the certificate that you created for your friendly DNS name.

6. If an error results when the installer registers a service principal name (SPN), manually create a Kerberos SPN for the DNS name. The SPN allows Integrated Windows Authentication between the browser and the AD FS IIS instance to work correctly:

```
setspn -a HOST/adfs.testzone.local testzone\ADFSSVR01
```

```
setspn -a HOST/adfs testzone\ADFSSVR01
```

For more information on Kerberos SPNs, see Active Directory and Kerberos SPNs Made Easy.

Configure Salesforce

To build a federation between two parties, you must establish a trust relationship by exchanging metadata. The metadata for the AD FS 2.0 instance is entered into the Salesforce configuration. Salesforce metadata is downloaded as an XML file that AD FS 2.0 can consume.

You have two things to configure: the domain and the SAML 2.0 setup.

Enable and Deploy My Domain on Your Salesforce Org

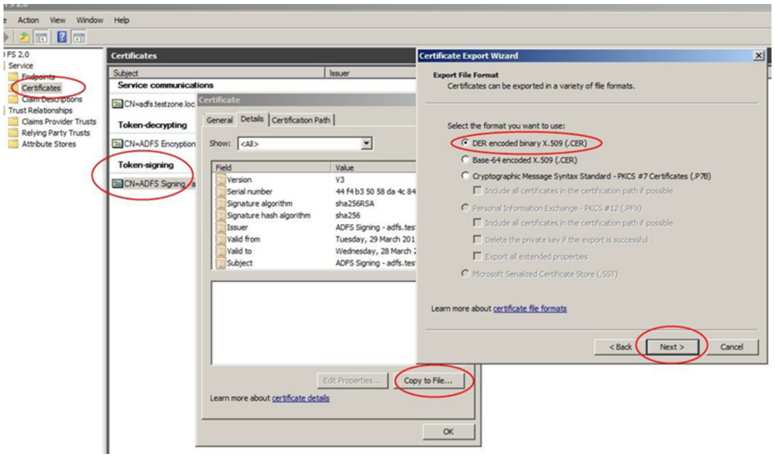
The Salesforce My Domain feature allows you to select a custom domain name for your application. A My Domain URL looks like https://customer.my.salesforce.com/ (for a production org) or https://customer-developer-edition.my.salesforce.com/ (for a Developer Edition).

A benefit of configuring My Domain is that it enables support for SP-initiated SSO. Configuring My Domain improves the user experience, allowing users to access deep links into their environment via SSO.

Use the My Domain wizard to set up a Salesforce subdomain.

Configure SAML 2.0

In the AD FS 2.0 MMC snap-in, select the certificates node, and double-click the token-signing certificate to view it. Click the **Details** tab and then select **Copy to File**. Save the certificate in DER format.



Field	Value
Version	V3
Serial number	44 f4 b3 50 58 da 4c 84
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ADFS Signing - adfs.tes
Valid from	Tuesday, 29 March 201
Valid to	Wednesday, 28 March 2
Subject	ADFS Signing - adfs.tes

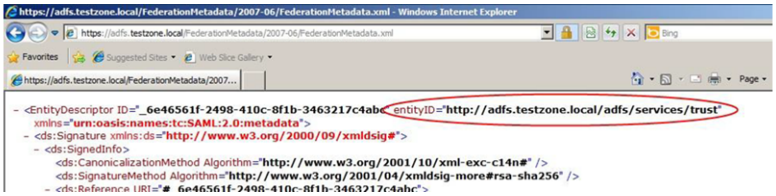
Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Delete the private key if the export is successful
□ Export all extended properties
○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

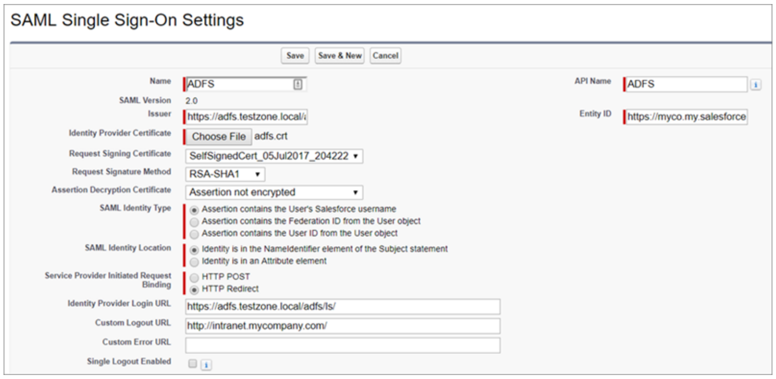
On the AD FS server, browse to the federation metadata URL located in the AD FS MMC at **Service** > **Endpoints** > **Metadata** > **Type:Federation Metadata**. In the example, the URL is https://adfs.testzone.local/FederationMetadata/2007-06/FederationMetadata.xml.


https://adfs.testzone.local/FederationMetadata/2007-06/FederationMetadata.xml - Windows Internet Explorer
https://adfs.testzone.local/FederationMetadata/2007-06/FederationMetadata.xml
Bing
Favorites
Suggested Sites
Web Slice Gallery
https://adfs.testzone.local/FederationMetadata/2007...
Page

```
- <EntityDescriptor ID="_6e46561f-2498-410c-8f1b-3463217c4abc" entityID="http://adfs.testzone.local/adfs/services/trust"
   xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
 - <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  - <ds:SignedInfo>
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
     <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
   - <ds:Reference URI="#_6e46561f-2498-410c-8f1b-3463217c4abc">
```

Copy the value of the entityID attribute. In the example, it is http://adfs.testzone.local.

In Salesforce, from Setup, enter `Single Sign-On` in the Quick Find box and select **Single Sign-On Settings**. Select **SAML Enabled**, and click the option to create a new SAML SSO configuration.



SAML Single Sign-On Settings

Name	ADFS	API Name	ADFS
SAML Version	2.0	Entity ID	https://myco.my.salesforce
Issuer	https://adfs.testzone.local/		
Identity Provider Certificate	Choose File adfs.crt		
Request Signing Certificate	SelfSignedCert_05Jul2017_204222		
Request Signature Method	RSA-SHA1		
Assertion Decryption Certificate	Assertion not encrypted		
SAML Identity Type	● Assertion contains the User's Salesforce username ○ Assertion contains the Federation ID from the User object ○ Assertion contains the User ID from the User object		
SAML Identity Location	● Identity is in the NameIdentifier element of the Subject statement ○ Identity is in an Attribute element		
Service Provider Initiated Request Binding	○ HTTP POST ● HTTP Redirect		
Identity Provider Login URL	https://adfs.testzone.local/adfs/ls/		
Custom Logout URL	http://intranet.mycompany.com/		
Custom Error URL			
Single Logout Enabled	□		

Configure the settings.

- **Name**—Enter a name for the SAML SSO settings.
- **SAML Version**—This setting is set to **2.0**.
- **Issuer**—Paste your entityID here.
- **Identity Provider Certificate**—Browse and select the token-signing certificate you exported earlier.
- **Request Signing Certificate**—Select a self-signed certificate you created earlier. (See the procedure for generating a self-signed certificate.)
- **Request Signature Method**—Set this setting to RSA-SHA-1.
- **SAML Identity Type**—To log in a user, you can match against either the Salesforce username or the federation ID. If matching the federation ID, it must be populated in the profile of every user. For testing, select federation ID. If users use their email address as their Salesforce username, a production deployment can switch to matching against the username.
- **SAML Identity Location**—To log in the user, you can use either the NameID in the SAML assertion or another attribute. You can use NameID, because AD FS populates NameID in the SAML assertion.
- **Service Provider Initiated Request Binding**—It's recommended that you choose **HTTP Redirect**.
- **Identity Provider Login URL**—Enter the URL of your AD FS SAML endpoint, to which Salesforce sends SAML requests for SP-initiated login.

  Note: Include the slash at the end of the URL.

  You can find the URL in the AD FS MMC at **Endpoints** > **Token Issuance** > **Type:SAML 2.0/WS-Federation**. In the example, the URL is https://adfs.testzone.local/adfs/ls/.

- **Identity Provider Logout URL**—You can configure a URL to which the user is sent after logging out, for example, http://intranet.mycompany.com/.
- **Entity ID**—This setting specifies how the AD FS IdP identifies the Salesforce SP. To enable SP-initiated SSO, enter the entity ID from your configured My Domain.

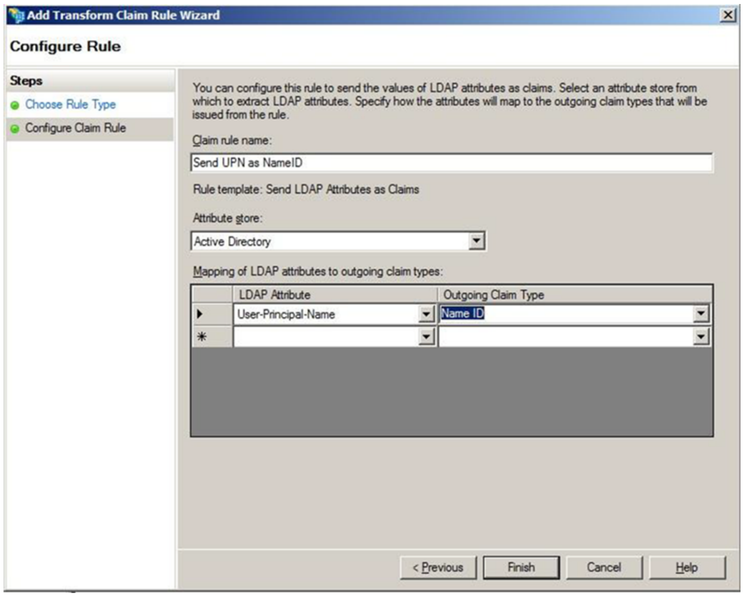
Save the settings, and download the metadata XML file.

AD FS 2.0 Configuration

Now that you have Salesforce metadata, create the AD FS side of the trust relationship. Open the AD FS 2.0 MMC snap-in, and add a new "Relying Party Trust."

- **Select Data Source**—Import data about a relying party from a file. Browse to the XML file that you downloaded from Salesforce.
- **Specify Display Name**—Give the trust a display name, such as `Salesforce Test`.
- **Choose Issuance Authorization Rules**—Permit all users to access this relying party.
- **Open Edit Claim Rules Dialog**—Select.

In the claim rules editor, click the **Issuance Transform Rules** tab. Add a rule using the **Claim Rule Template** set to **Send LDAP Attributes as Claims**.



You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: Send UPN as NameID

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
▶	User-Principal-Name	Name ID
*		

- **Claim Rule Name**—For testing, set the attribute **User-Principal-Name** as `NameID`, and call the rule `Send UPN as NameID`. In production, it's common to send the user's email address or employee ID. It's important to use an attribute with a value that is unlikely to change over time, because any change invalidates SSO for that user.
- **LDAP Attribute**—Select **User Principal Name**.
- **Outgoing Claim Type**—Select **Name ID**.

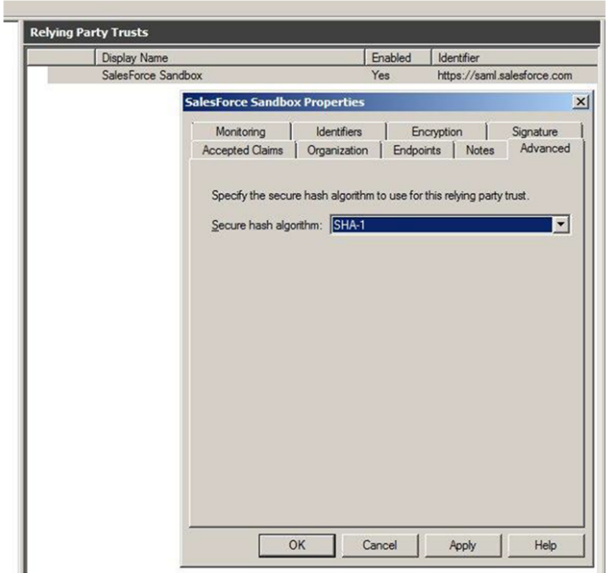
SP-Initiated Login

With an IdP-initiated login process, you typically set up a link on the company intranet that users click to get access to Salesforce. SP-initiated login happens when a user clicks a direct link to Salesforce.

If you configured a My Domain entity ID in the Salesforce SAML settings (for example, https://testinfo-developer-edition.my.salesforce.com), users can go to URLs in that domain. They are then redirected to AD FS for authentication.

For an SP-initiated login to work, set the AD FS secure hash algorithm parameter to SHA-1. Salesforce uses SHA-1 when signing SAML requests, and AD FS defaults to SHA-256.

The SHA parameter is set in the AD FS trust properties for the Salesforce relying party on the Advanced tab.



Display Name	Enabled	Identifier
SalesForce Sandbox	Yes	https://saml.salesforce.com

Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-1

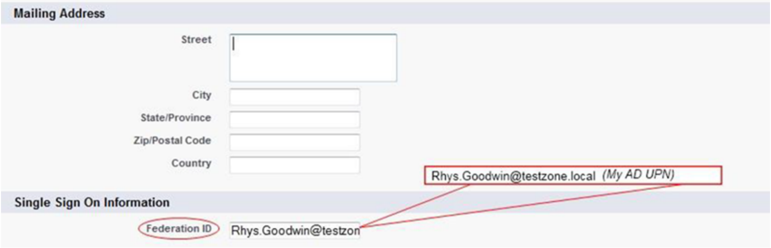
If you don't set this parameter, you get a message in the AD FS event log.

```
Event ID: 378
```

```
SAML request is not signed with expected signature algorithm. SAML request is signed with
 signature algorithm http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 . Expected signature
 algorithm is http://www.w3.org/2000/09/xmldsig#rsa-sha1
```

Testing

You can now set the federation ID of a Salesforce user to the UPN of the AD user account and test the login process.



Mailing Address

Street	
City	
State/Province	
Zip/Postal Code	
Country	

Single Sign On Information

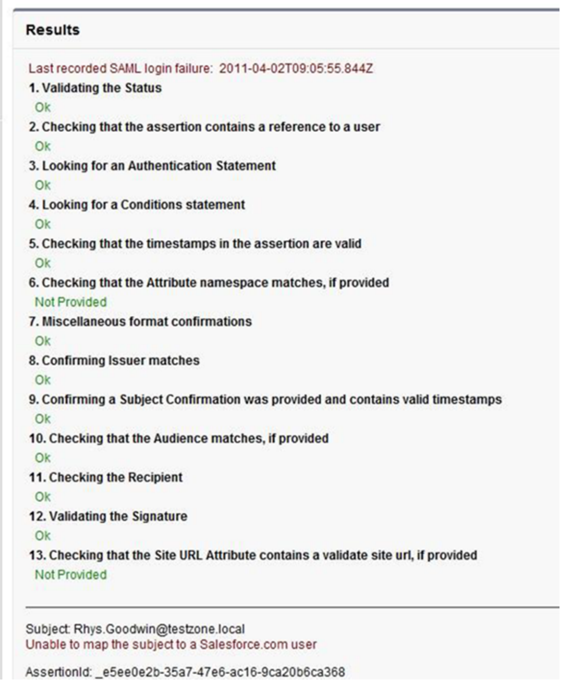
Federation ID: Rhys.Goodwin@testzon

Rhys.Goodwin@testzone.local

For SP-initiated login, assuming you configured a My Domain entity ID, browse straight to the URL, for example, https://testinfo-developer-edition.my.salesforce.com.

For IdP-initiated login, use the AD FS login URL and specify the loginToRp parameter as the Salesforce SAML entity ID, for example, https://adfs.testzone.local/adfs/ls/idpinitiatedsignon.aspx?loginToRp=https://saml.salesforce.com.

In either case, the browser follows a chain of redirects, ultimately logging you in to your application on Salesforce. If you get a Salesforce login error, use the SAML assertion validator tool on the Salesforce SSO configuration page. It displays the results of the last failed SAML login.



```
Results

Last recorded SAML login failure:  2011-04-02T09:05:55.844Z
1. Validating the Status
  Ok
2. Checking that the assertion contains a reference to a user
  Ok
3. Looking for an Authentication Statement
  Ok
4. Looking for a Conditions statement
  Ok
5. Checking that the timestamps in the assertion are valid
  Ok
6. Checking that the Attribute namespace matches, if provided
  Not Provided
7. Miscellaneous format confirmations
  Ok
8. Confirming Issuer matches
  Ok
9. Confirming a Subject Confirmation was provided and contains valid timestamps
  Ok
10. Checking that the Audience matches, if provided
  Ok
11. Checking the Recipient
  Ok
12. Validating the Signature
  Ok
13. Checking that the Site URL Attribute contains a validate site url, if provided
  Not Provided

Subject: Rhys.Goodwin@testzone.local
Unable to map the subject to a Salesforce.com user

AssertionId: _e5ee0e2b-35a7-47e6-ac16-9ca20b6ca368
```

If you get an error from AD FS, check the AD FS logs in Server Manager\Diagnostics\Applications and Services Logs\AD FS 2.0\Admin. There is also a good MSDN blog post on AD FS 2.0 diagnostics.

If you configured a My Domain entity ID, SP-initiated login works for deep-links. Bookmark a link from deep inside Salesforce and then log out. Reload your browser, and select the bookmark. You are redirected to your IdP, authenticated, and then redirected back to the bookmarked link.

Common Issues and Troubleshooting

- Federation ID is case-sensitive.

  If the federated identity is your organizational email address, be sure to enter it exactly as AD FS sends it. Otherwise, Salesforce cannot find a matching user.

  Unfortunately, you can't write a custom claim rule to normalize the case of the LDAP attribute before sending it because the claims language has only a basic regular expression replace.

- Assertion has expired.

  Assertions with a timestamp more than 5 minutes old are rejected.

  > Note: Salesforce does make an allowance of 3 minutes for clock skew. Therefore, an assertion can be as much as 8 minutes past the timestamp time or 3 minutes before it. This amount of time is less if the assertion's validity period is less than 5 minutes.

  Ensure that your AD FS server's system clock is synchronized to a good internet time source using Network Time Protocol (NTP).

- Prevented from logging in to Salesforce.

  If a configuration error prevents you from logging in to Salesforce via SSO, you can still log in via username and password. Append `?login` to the login URL, for example, https://login.salesforce.com/?login or https://testinfo-developer-edition.my.salesforce.com/?login. After logging in, you can disable SSO if necessary while you troubleshoot the issue.

SEE ALSO:

Single Sign-On

Best Practices for Implementing Single Sign-On

The Elements of User Authentication

Single Sign-On Implementation Guide

Salesforce Security Developer Center

Microsoft blog: A Quick Walkthrough: Setting up AD FS SAML Federation with a Shibboleth SP

Microsoft blog: Using Federation Metadata to Establish a Relying Party Trust in AD FS 2.0

Configure Remote Site Settings

Before any Visualforce page, Apex callout, or JavaScript code using XmlHttpRequest in an s-control or custom button can call an external site, that site must be registered in the Remote Site Settings page, or the call fails.

Note: To enable corresponding access for Lightning components, create a CSP Trusted Site.

To access the page, from Setup, enter *Remote Site Settings* in the `Quick Find` box, then select **Remote Site Settings**. This page displays a list of any remote sites already registered and provides additional information about each site, including remote site name and URL.

For security reasons, Salesforce restricts the outbound ports you may specify to one of the following:

- 80: This port only accepts HTTP connections.
- 443: This port only accepts HTTPS connections.
- 1024–66535 (inclusive): These ports accept HTTP or HTTPS connections.

To register a new site:

1. Click **New Remote Site**.
2. Enter a descriptive term for the `Remote Site Name`.
3. Enter the URL for the remote site.
4. To allow access to the remote site regardless of whether the user's connection is over HTTP or HTTPS, select the `Disable Protocol Security` checkbox. When selected, Salesforce can pass data from an HTTPS session to an HTTP session, and vice versa. Only select this checkbox if you understand the security implications.
5. Optionally, enter a description of the site.
6. Click **Save** to finish, or click **Save & New** to save your work and begin registering an additional site.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Visualforce and S-controls are not available in **Database.com**

USER PERMISSIONS

To configure remote settings:

- Customize Application or Modify All Data

SEE ALSO:

Create CSP Trusted Sites to Access Third-Party APIs

Named Credentials

A named credential specifies the URL of a callout endpoint and its required authentication parameters in one definition. To simplify the setup of authenticated callouts, specify a named credential as the callout endpoint. If you instead specify a URL as the callout endpoint, you must register that URL in your org's remote site settings and handle the authentication yourself. For example, for an Apex callout, your code would need to handle authentication, which can be less secure and especially complicated for OAuth implementations.

Salesforce manages all authentication for callouts that specify a named credential as the callout endpoint so that you don't have to. You can also skip remote site settings, which are otherwise required for callouts to external sites, for the site defined in the named credential.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

Named credentials are supported in these types of callout definitions:

- Apex callouts
- External data sources of these types:
  - Salesforce Connect: OData 2.0
  - Salesforce Connect: OData 4.0
  - Salesforce Connect: Custom (developed with the Apex Connector Framework)

By separating the endpoint URL and authentication from the callout definition, named credentials make callouts easier to maintain. For example, if an endpoint URL changes, you update only the named credential. All callouts that reference the named credential simply continue to work.

If you have multiple orgs, you can create a named credential with the same name but with a different endpoint URL in each org. You can then package and deploy—on all the orgs—one callout definition that references the shared name of those named credentials. For example, the named credential in each org can have a different endpoint URL to accommodate differences in development and production environments. If an Apex callout specifies the shared name of those named credentials, the Apex class that defines the callout can be packaged and deployed on all those orgs without programmatically checking the environment.

Named credentials support basic password authentication and OAuth 2.0. You can set up each named credential to use an org-wide named principal or to use per-user authentication so that users can manage their own credentials.

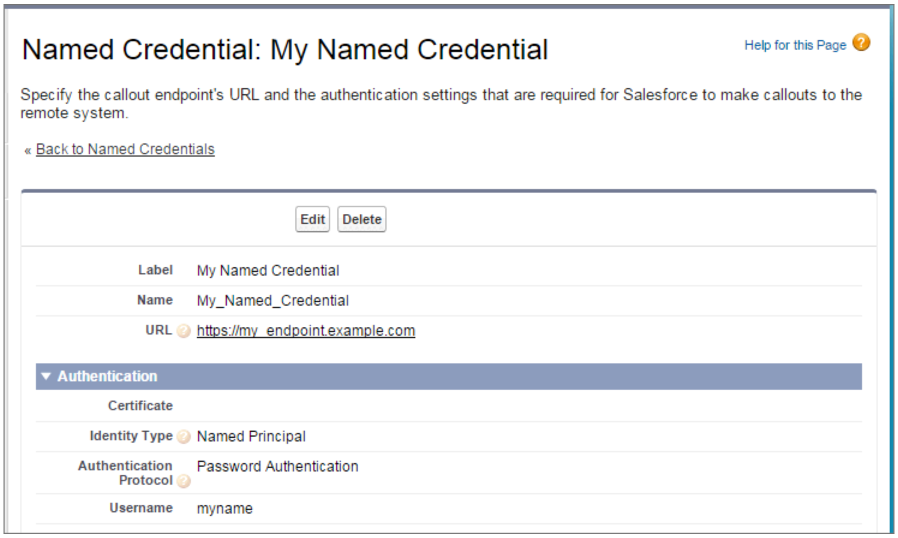
To reference a named credential from a callout definition, use the named credential URL. A named credential URL contains the scheme `callout:`, the name of the named credential, and an optional path. For example: `callout:`*My_Named_Credential/some_path*.

You can append a query string to a named credential URL. Use a question mark (?) as the separator between the named credential URL and the query string. For example: `callout:`*My_Named_Credential/some_path*`?format=json`.

Example: In the following Apex code, a named credential and an appended path specify the callout's endpoint.

```
HttpRequest req = new HttpRequest();
req.setEndpoint('callout:My_Named_Credential/some_path');
req.setMethod('GET');
Http http = new Http();
HTTPResponse res = http.send(req);
System.debug(res.getBody());
```

The referenced named credential specifies the endpoint URL and the authentication settings.



Named Credential: My Named Credential

Specify the callout endpoint's URL and the authentication settings that are required for Salesforce to make callouts to the remote system.

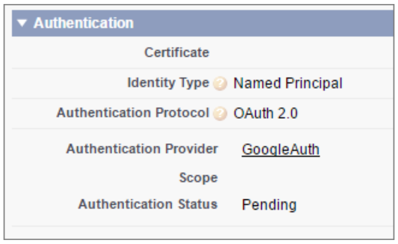
« Back to Named Credentials

Label	My Named Credential
Name	My_Named_Credential
URL	https://my_endpoint.example.com

Authentication

Certificate	
Identity Type	Named Principal
Authentication Protocol	Password Authentication
Username	myname

If you use OAuth instead of password authentication, the Apex code remains the same. The authentication settings differ in the named credential, which references an authentication provider that's defined in the org.



Authentication

Certificate	
Identity Type	Named Principal
Authentication Protocol	OAuth 2.0
Authentication Provider	GoogleAuth
Scope	
Authentication Status	Pending

In contrast, let's see what the Apex code looks like without a named credential. Notice that the code becomes more complex to handle authentication, even if we stick with basic password authentication. Coding OAuth is even more complex and is an ideal use case for named credentials.

```
HttpRequest req = new HttpRequest();
req.setEndpoint('https://my_endpoint.example.com/some_path');
req.setMethod('GET');

// Because we didn't set the endpoint as a named credential,
// our code has to specify:
// - The required username and password to access the endpoint
// - The header and header information

String username = 'myname';
String password = 'mypwd';

Blob headerValue = Blob.valueOf(username + ':' + password);
String authorizationHeader = 'BASIC ' +
EncodingUtil.base64Encode(headerValue);
req.setHeader('Authorization', authorizationHeader);

// Create a new http object to send the request object
// A response object is generated as a result of the request

Http http = new Http();
HTTPResponse res = http.send(req);
System.debug(res.getBody());
```

IN THIS SECTION:

Define a Named Credential

Create a named credential to specify the URL of a callout endpoint and its required authentication parameters in one definition. You can then specify the named credential as a callout endpoint to let Salesforce handle all the authentication. You can also skip remote site settings, which are otherwise required for callouts to external sites, for the site defined in the named credential.

Grant Access to Authentication Settings for Named Credentials

For named credentials that use per-user authentication, grant access to users through permission sets and profiles. Doing so lets users set up and manage their own authentication settings for accessing the external system.

SEE ALSO:

Define a Named Credential

Grant Access to Authentication Settings for Named Credentials

Apex Developer Guide : Invoking Callouts Using Apex

External Authentication Providers

Define a Named Credential

Create a named credential to specify the URL of a callout endpoint and its required authentication parameters in one definition. You can then specify the named credential as a callout endpoint to let Salesforce handle all the authentication. You can also skip remote site settings, which are otherwise required for callouts to external sites, for the site defined in the named credential.

Named credentials are supported in these types of callout definitions:

- Apex callouts
- External data sources of these types:
  - Salesforce Connect: OData 2.0
  - Salesforce Connect: OData 4.0
  - Salesforce Connect: Custom (developed with the Apex Connector Framework)

To set up a named credential:

1. From Setup, enter `Named Credentials` in the `Quick Find` box, then select **Named Credentials**.
2. Click **New Named Credential**, or click **Edit** to modify an existing named credential.
3. Complete the fields.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To view named credentials:

- View Setup and Configuration

To create, edit, or delete named credentials:

- Customize Applications

Field	Description
`Label`	A user-friendly name for the named credential that's displayed in the Salesforce user interface, such as in list views. If you set `Identity Type` to Per User, this label appears when your users view or edit their authentication settings for external systems.
`Name`	A unique identifier that's used to refer to this named credential from callout definitions and through the API. The name can contain only underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.

`URL`	The URL or root URL of the callout endpoint. Must begin with *`http://`* or *`https://`*. Can include a path but not a query string. Examples:
	- `http://my_endpoint.example.com`
	- `https://my_endpoint.example.com/secure/payroll`
	You can, however, append a query string and a specific path in the callout definition's reference to the named credential. For example, an Apex callout could reference the named credential "My_Payroll_System" as follows.
	`HttpRequest req = new HttpRequest();`
	`req.setEndpoint('callout:My_Payroll_System/paystubs?format=json');`

`Certificate`	If you specify a certificate, your Salesforce org supplies it when establishing each two-way SSL connection with the external system. The certificate is used for digital signatures, which verify that requests are coming from your Salesforce org.
`Identity Type`	Determines whether you're using one set or multiple sets of credentials to access the external system. - Anonymous: No identity and therefore no authentication. - Per User: Use separate credentials for each user who accesses the external system via callouts. Select this option if the external system restricts access on a per-user basis. After you grant user access through permission sets or profiles in Salesforce, users can manage their own authentication settings for external systems in their personal settings. - Named Principal: Use the same set of credentials for all users who access the external system from your org. Select this option if you designate one user account on the external system for all your Salesforce org users.

4. Select the authentication protocol.
    - If you select **Password Authentication**, enter the username and password for accessing the external system.
    - If you select **OAuth 2.0**, complete the following fields.

Field	Description
`Authentication Provider`	Choose the provider. See External Authentication Providers on page 670.
`Scope`	Specifies the scope of permissions to request for the access token. Your authentication provider determines the allowed values. See Use the Scope Parameter on page 699. Note: – The value that you enter replaces the `Default Scopes` value that's defined in the specified authentication provider. – Whether scopes are defined can affect whether each OAuth flow prompts the user with a consent screen. – We recommend that you request a refresh token or offline access. Otherwise, when the token expires, you lose access to the external system.
`Start Authentication Flow on Save`	To authenticate to the external system and obtain an OAuth token, select this checkbox. This authentication process is called an OAuth flow. When you click **Save**, the external system prompts you to log in. After successful login, the external system grants you an OAuth token for accessing its data from this org. Redo the OAuth flow when you need a new token—for example, if the token expires—or if you edit the `Scope` or `Authentication Provider` fields.

5. If you want to use custom headers or bodies in the callouts, enable the relevant options.

Field	Description
`Generate Authorization Header`	By default, Salesforce generates an authorization header and applies it to each callout that references the named credential. Deselect this option only if one of the following statements applies. • The remote endpoint doesn't support authorization headers. • The authorization headers are provided by other means. For example, in Apex callouts, the developer can have the code construct a custom authorization header for each callout. This option is required if you reference the named credential from an external data source.

`Allow Merge Fields in HTTP Header`
`Allow Merge Fields in HTTP Body`
	In each Apex callout, the code specifies how the HTTP header and request body are constructed. For example, the Apex code can set the value of a cookie in an authorization header.
	These options enable the Apex code to use merge fields to populate the HTTP header and request body with org data when the callout is made.
	These options aren't available if you reference the named credential from an external data source.

To reference a named credential from a callout definition, use the named credential URL. A named credential URL contains the scheme `callout:`, the name of the named credential, and an optional path. For example: `callout:`*`My_Named_Credential`*`/`*`some_path`*.

You can append a query string to a named credential URL. Use a question mark (?) as the separator between the named credential URL and the query string. For example: `callout:`*`My_Named_Credential`*`/`*`some_path`*`?format=json`.

SEE ALSO:

Named Credentials

Grant Access to Authentication Settings for Named Credentials

Apex Developer Guide : Invoking Callouts Using Apex

Grant Access to Authentication Settings for Named Credentials

For named credentials that use per-user authentication, grant access to users through permission sets and profiles. Doing so lets users set up and manage their own authentication settings for accessing the external system.

1. From Setup, enter *`Permission Sets`* in the `Quick Find` box, then select **Permission Sets** or **Profiles**.
2. Click the name of the permission set or profile that you want to modify.
3. Do one of the following.
   - For a permission set, or for a profile in the enhanced profile user interface, click **Named Credential Access** in the Apps section. Then click **Edit**.
   - For a profile in the original profile user interface, click **Edit** in the Enabled Named Credential Access section.
4. Add the named credentials that you want to enable.
5. Click **Save**.

SEE ALSO:

Store Authentication Settings for External Systems

Define a Named Credential

Named Credentials

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in all editions

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

USER PERMISSIONS

To edit permission sets and user profiles:

- Manage Profiles and Permission Sets

Identity Connect

Identity Connect integrates Microsoft Active Directory (AD) with Salesforce. User information entered in AD is shared with Salesforce seamlessly and instantaneously. Companies that use AD for user management can use Identity Connect to manage Salesforce accounts.

Changes in AD are reflected in Salesforce in near real time. For example, when a user is created in AD, the Salesforce user account is created as part of the provisioning process. When deprovisioned, the user's Salesforce session is revoked immediately.

You can also use Identity Connect for single sign-on to Salesforce.

Identity Connect runs as a service on either Windows or Linux platforms.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available for an additional cost in: **Enterprise**, **Performance**, and **Unlimited** Editions. **Developer** Edition includes 10 Identity Connect permission set licenses.

IN THIS SECTION:

- Installing Identity Connect
- Enabling Identity Connect

SEE ALSO:

- Installing Identity Connect
- Enabling Identity Connect
- Identity Connect Implementation Guide

Installing Identity Connect

Your organization must have at least one Identity Connect license. To obtain Identity Connect, contact Salesforce.

The Identity Connect software will typically be installed on a server by your IT department. Each user does not need to install Identity Connect individually.

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

   Note: **Identity Connect** doesn't appear in Setup until Salesforce adds the feature to your organization.

2. Click the download link that corresponds to your operating system.
3. Install the software according to the Salesforce Identity Connect Implementation Guide.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available for an additional cost in: **Enterprise**, **Performance**, and **Unlimited** Editions. **Developer** Edition includes 10 Identity Connect permission set licenses.

USER PERMISSIONS

To install Identity Connect:

- Manage Users

SEE ALSO:

- Identity Connect
- Enabling Identity Connect

Enabling Identity Connect

To obtain Identity Connect, contact Salesforce.

To enable Identity Connect for a user:

1. Assign the Identity Connect license to the user.
2. Create a permission set and add the "Use Identity Connect" permission to it.
3. Assign the permission set to the user.

SEE ALSO:

Identity Connect

Installing Identity Connect

Identity Connect Implementation Guide

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available for an additional cost in: **Enterprise**, **Performance**, and **Unlimited** Editions. **Developer** Edition includes 10 Identity Connect permission set licenses.

USER PERMISSIONS

To assign a permission set license:

- Manage Internal Users

To create and assign permission sets:

- Manage Profiles and Permission Sets

To view users that are assigned to a permission set:

- View Setup and Configuration

Single Logout

With single logout (SLO), your users log out from one application, and are automatically logged out from other applications they are using.

For example, when Salesforce is the identity provider for connected applications, the user logs out from Salesforce and is automatically logged out of the other applications. Or, when a user is logged in to Salesforce from an identity provider using SAML, the user logs out of Salesforce and is automatically logged out of the identity provider, too. SLO can improve security and usability. Previously, your users had to remember to log out of each app separately.

To use SLO, the identity provider, service providers, and relying parties must be configured for single sign-on and registered for SLO.

Salesforce supports front-channel SLO, meaning your users are only logged out of their registered apps if they explicitly log out of one using their browsers. Having a session expire doesn't cause them to be logged out of the other apps registered for SLO.

Salesforce supports the following protocols:

- SAML SLO as an identity provider or service provider, initiated by either.
- OpenID Connect SLO as an identity provider or relying party, initiated by either.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Modify All Data

Examples:

1. You want users to log in to Salesforce, then use connected apps to log in to other services. When they're ready to log out, they log out from Salesforce (or a configured service provider or relying party) and they're automatically logged out of all the configured connected apps and services. This behavior can be accomplished with the following:
   - SAML SLO for which Salesforce is the identity provider, and registered SAML connected apps are service providers
   - OpenID Connect SLO for which Salesforce is the identity provider, and registered OAuth connected apps are relying parties
2. You want users to log in to Salesforce using an external identity provider. The identity provider uses SAML or OpenID Connect to log the users in to a Salesforce org. When the users log out of the identity provider (or Salesforce) session, they're automatically logged out of both. This behavior can be accomplished with the following:
   - SAML SLO when Salesforce is the service provider connected to an external SAML identity provider
   - OpenID Connect SLO when Salesforce is the relying party connected to an external OpenID Connect provider

Implementing SLO brings several advantages to your org.

- Time savings—With SLO in place, users avoid manually logging out of connected apps. Fewer steps and no toggling through various apps saves time and reduces frustration.
- Increased security—Users don't have to remember to log out of any connected apps. When they log out of Salesforce, they are also logged out of the other apps. Even if a user leaves a desktop unattended, nobody can access these apps

IN THIS SECTION:

Configure SAML Settings for Single Logout Where Salesforce Is the Service Provider

Configure SLO when Salesforce is the service provider connected to an external SAML identity provider. Users log in to an identity provider. The identity provider uses SAML to log the users in to a Salesforce org. When the users log out of the identity provider (or Salesforce) session, they're automatically logged out of both.

Configure SAML Settings for Single Logout Where Salesforce Is the Identity Provider

Configure SLO when Salesforce is the identity provider connected to an external SAML service provider. Users log in to Salesforce. Salesforce uses SAML to log in users to the service provider through a connected app. When the users log out of the service provider (or Salesforce) session, they're automatically logged out of both.

Configure OpenID Connect Settings for Single Logout Where Salesforce Is the Relying Party

Configure SLO when authentication providers use OpenID Connect to give users access to Salesforce as the relying party. Users log in to Salesforce through the authentication provider. When the users log out of Salesforce (or the authentication provider) session, they're automatically logged out of both.

Configure OpenID Connect Settings for Single Logout Where Salesforce Is the OpenID Connect Provider

Configure SLO when Salesforce provides authentication for users to access a relying provider using OpenID Connect. Users log in to Salesforce. Salesforce uses OpenID Connect to authenticate users for the relying party through a connected app. When the users log out of the relying party (or Salesforce) session, they're automatically logged out of both.

Configure SAML Settings for Single Logout Where Salesforce Is the Service Provider

Configure SLO when Salesforce is the service provider connected to an external SAML identity provider. Users log in to an identity provider. The identity provider uses SAML to log the users in to a Salesforce org. When the users log out of the identity provider (or Salesforce) session, they're automatically logged out of both.

To use this feature:

- Enable My Domain.
- Get the Issuer URL from the identity provider. This URL uniquely identifies your SAML identity provider. SAML assertions sent to Salesforce must match this value exactly in the `<saml:Issuer>` attribute of SAML assertions.
- Get and save the certificate for validating signatures from the identity provider.
- Get the single logout URL from the identity provider.

Note: Some identity providers don't support logout initiated by the service provider. In this case, do only step 6. Users will be able to log out of Salesforce when initiated by the identity provider. But, logging out of Salesforce won't necessarily log the user out of the identity provider session.

1. In Setup, enter *`Single Sign-On Settings`* in the `Quick Find` box, then select **Single Sign-On Settings**.
2. In SAML Single Sign-On Settings, select **New**.
3. On the **SAML Single Sign-On Settings** page, enter the required information and select **Single Logout Enabled**.
4. For **Identity Provider Single Logout URL**, enter the SAML SLO endpoint of the identity provider. This URL is the endpoint where Salesforce sends LogoutRequests (when a logout is initiated by Salesforce), or LogoutResponses (when a logout is initiated by the identity provider). The identity provider gives you this endpoint.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Federated Authentication is available in: **All** Editions

Delegated Authentication is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Authentication Providers are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view the settings:

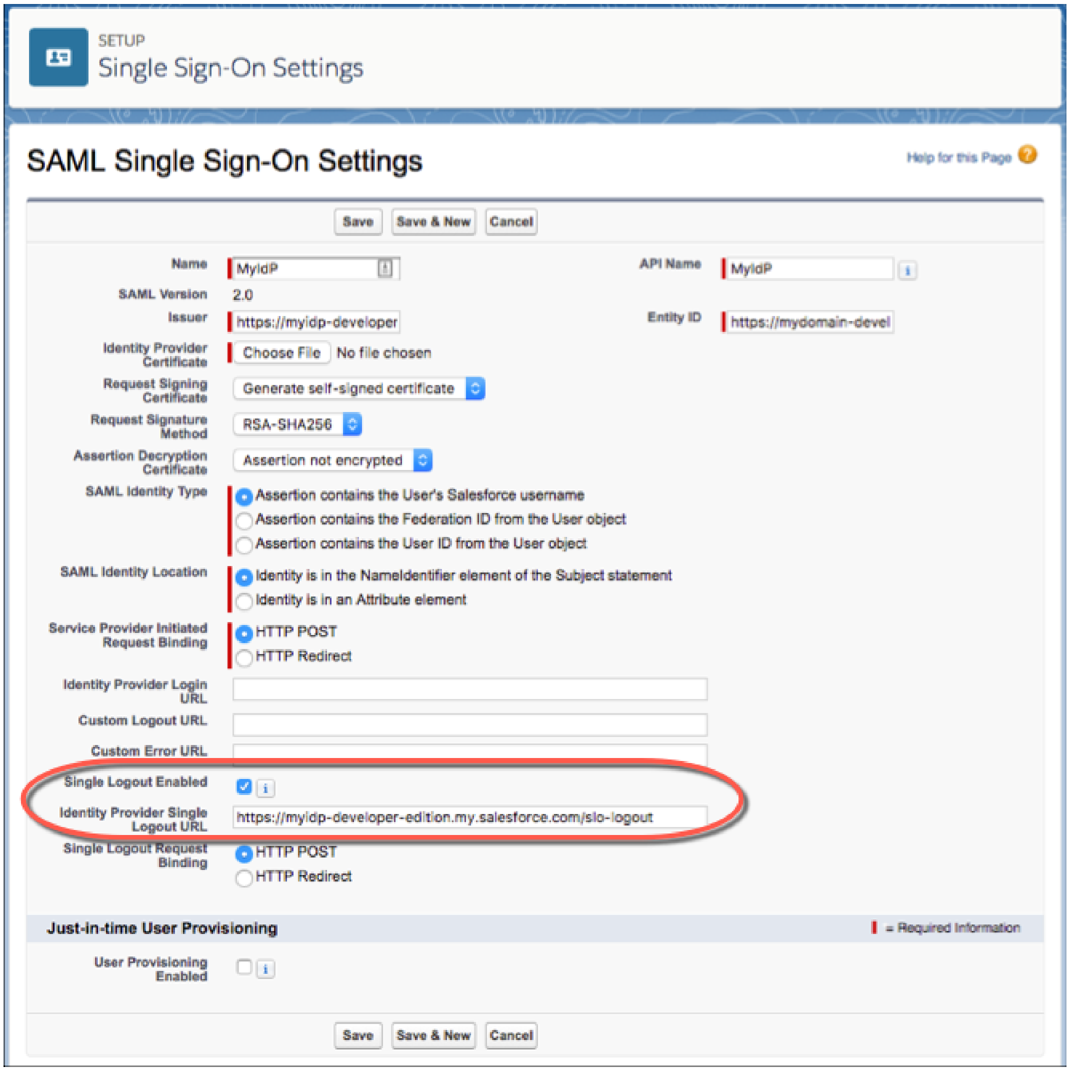
- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Modify All Data



SETUP

Single Sign-On Settings

SAML Single Sign-On Settings

Name: MyIdP

API Name: MyIdP

SAML Version: 2.0

Issuer: https://myidp-developer

Entity ID: https://mydomain-devel

Identity Provider Certificate: Choose File No file chosen

Request Signing Certificate: Generate self-signed certificate

Request Signature Method: RSA-SHA256

Assertion Decryption Certificate: Assertion not encrypted

SAML Identity Type:
● Assertion contains the User's Salesforce username
○ Assertion contains the Federation ID from the User object
○ Assertion contains the User ID from the User object

SAML Identity Location:
● Identity is in the NameIdentifier element of the Subject statement
○ Identity is in an Attribute element

Service Provider Initiated Request Binding:
● HTTP POST
○ HTTP Redirect

Identity Provider Login URL:

Custom Logout URL:

Custom Error URL:

Single Logout Enabled: ☑

Identity Provider Single Logout URL: https://myidp-developer-edition.my.salesforce.com/slo-logout

Single Logout Request Binding:
● HTTP POST
○ HTTP Redirect

Just-in-time User Provisioning

= Required Information

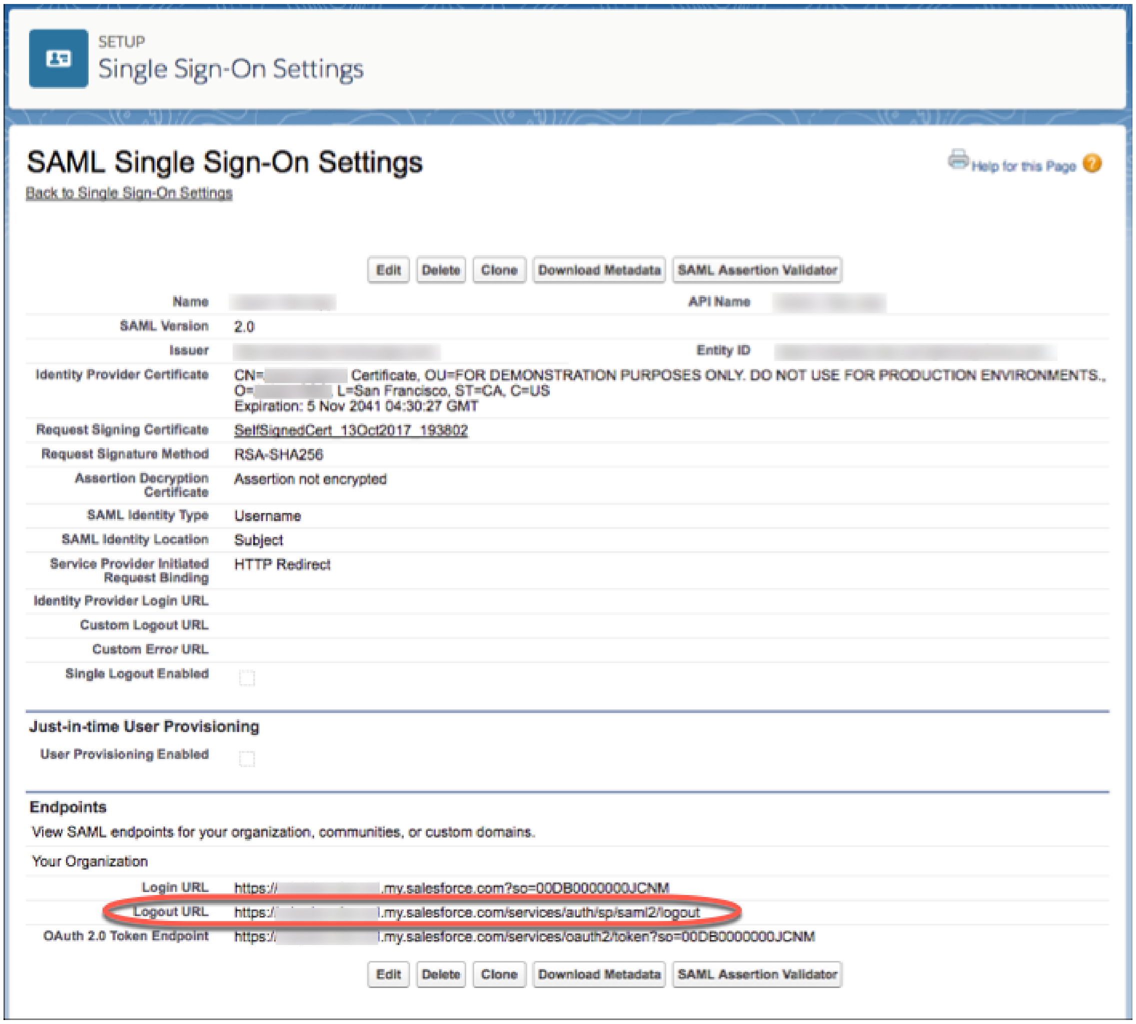
User Provisioning Enabled: □

5. Select the HTTP binding type to be used for service provider-initated SLO. The binding type determines where to put the LogoutRequest or LogoutResponse in the SAML request. The value is base64 encoded.

   HTTP Redirect — Sent in the querystring, deflated.

   HTTP POST — Sent in the POST body, not deflated.

6. Provide your IdP with the Salesforce SP SLO endpoint. It is the **Logout URL** found under Your Organization in Endpoints on the **SAML Single Sign-On Settings** page. The format for the endpoint is `https://<domain>.my.salesforce.com/services/auth/sp/saml2/logout`, where `<domain>` is your org's My Domain name.



SAML Single Sign-On Settings

Back to Single Sign-On Settings

Name	[redacted]	API Name	[redacted]
SAML Version	2.0		
Issuer	[redacted]	Entity ID	[redacted]
Identity Provider Certificate	CN=[redacted] Certificate, OU=FOR DEMONSTRATION PURPOSES ONLY. DO NOT USE FOR PRODUCTION ENVIRONMENTS., O=[redacted], L=San Francisco, ST=CA, C=US Expiration: 5 Nov 2041 04:30:27 GMT		
Request Signing Certificate	SelfSignedCert_13Oct2017_193802		
Request Signature Method	RSA-SHA256		
Assertion Decryption Certificate	Assertion not encrypted		
SAML Identity Type	Username		
SAML Identity Location	Subject		
Service Provider Initiated Request Binding	HTTP Redirect		
Identity Provider Login URL			
Custom Logout URL			
Custom Error URL			
Single Logout Enabled	□		

Just-in-time User Provisioning

User Provisioning Enabled □

Endpoints

View SAML endpoints for your organization, communities, or custom domains.

Your Organization

Login URL	https://[redacted].my.salesforce.com?so=00DB0000000JCNM
Logout URL	https://[redacted].my.salesforce.com/services/auth/sp/saml2/logout
OAuth 2.0 Token Endpoint	https://[redacted].my.salesforce.com/services/oauth2/token?so=00DB0000000JCNM

If the org is a Salesforce Community, the Logout URL for the community appears on the same page.

SEE ALSO:

Single Logout

Configure SAML Settings for Single Logout Where Salesforce Is the Identity Provider

Configure SLO when Salesforce is the identity provider connected to an external SAML service provider. Users log in to Salesforce. Salesforce uses SAML to log in users to the service provider through a connected app. When the users log out of the service provider (or Salesforce) session, they're automatically logged out of both.

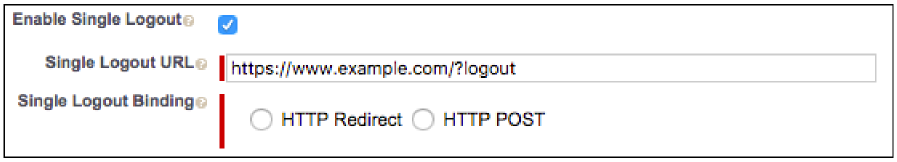
To use this feature:

- Enable My Domain.
- Make sure that the service provider supports SAML SLO.
- Get the SAML SLO endpoint from the service provider.
- Find out the HTTP binding type from the service provider.

Note: Some service providers don't support initiating single logout. In this case, skip step 6. Users are logged out of the service provider when initiated by Salesforce. But, logging out of the service provider won't necessarily log the user out of Salesforce.

This implementation uses connected apps. You can configure SLO when you create and edit a connected app as a developer, and distribute it to other orgs. Or, you can create and manage SLO for a connected app within your org as an administrator. Changes to the SLO configuration in the connected app management page are not propagated back to the page when you're editing a connected app as a developer. As you change settings through connected app management pages, manually copy settings to the app creation page, if desired.

1. For an existing connected app: In Setup, enter `apps` in the `Quick Find` box, then select **Manage Connected Apps**.
2. Next to the connected app that you want to configure for SLO, click **Edit**. You are now editing the connected app configuration, even though the path here was through **Manage Connected Apps**.
3. Under SAML Service Provider Settings, select **Enable Single Logout**.



Enable Single Logout ☑

Single Logout URL https://www.example.com/?logout

Single Logout Binding ○ HTTP Redirect ○ HTTP POST

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Federated Authentication is available in: **All** Editions

Delegated Authentication is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Authentication Providers are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Modify All Data

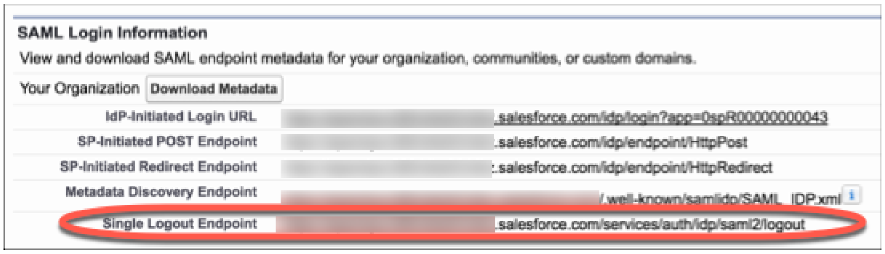
4. For Single Logout URL, enter the SAML SLO endpoint of the connected app service provider (SP). The URL must start with `https://`. This URL is the endpoint where Salesforce sends LogoutRequests (when a logout is initiated by Salesforce), or LogoutResponses (when a logout is initiated by the service provider). The service provider gives you this endpoint.
5. Select the HTTP binding type for SLO. The binding type determines where to put the LogoutRequest or LogoutResponse in the SAML request. The value is base64 encoded. The service provider gives you this information.

   HTTP Redirect — Sent in the querystring, deflated.

   HTTP POST — Sent in the POST body, not deflated.

6. Provide your service provider with the Salesforce identity provider SLO endpoint. With this endpoint, the service provider can initiate SLO. It's listed in the **Single Logout Endpoint** under SAML Login Information on the Connected App Detail page, and in the SAML Metadata Discovery Endpoint. The format for the endpoint is

https://<domain>.my.salesforce.com/services/auth/idp/saml2/logout, where *<domain>* is your org's My Domain name.



SAML Login Information

View and download SAML endpoint metadata for your organization, communities, or custom domains.

Your Organization

IdP-Initiated Login URL	[redacted].salesforce.com/idp/login?app=0spR00000000043
SP-Initiated POST Endpoint	[redacted].salesforce.com/idp/endpoint/HttpPost
SP-Initiated Redirect Endpoint	[redacted].salesforce.com/idp/endpoint/HttpRedirect
Metadata Discovery Endpoint	[redacted]/.well-known/samlidp/SAML_IDP.xml
Single Logout Endpoint	[redacted].salesforce.com/services/auth/idp/saml2/logout

SEE ALSO:

Single Logout

Configure OpenID Connect Settings for Single Logout Where Salesforce Is the Relying Party

Configure SLO when authentication providers use OpenID Connect to give users access to Salesforce as the relying party. Users log in to Salesforce through the authentication provider. When the users log out of Salesforce (or the authentication provider) session, they're automatically logged out of both.

To use this feature:

- Enable My Domain.
- Make sure that the authentication provider supports OpenID Connect SLO.
- Set up the authentication provider.
- Get the OpenID Connect SLO logout endpoint from the authentication provider.

> Note: Some authentication providers don't support logout initiated by the relying party. In this case, do only step 5. Users will be able to log out of Salesforce when initiated by the authentication provider. But, logging out of Salesforce won't necessarily log the user out of the authentication provider session.

1. In Setup, enter `Auth. Providers` in the **Quick Find** box, then select **Auth. Providers**.
2. Next to the auth provider that you want to configure for SLO, click **Edit**.
3. Under **Auth. Provider Edit**, enter the logout endpoint from the authentication provider in **Custom Logout URL**. With this endpoint, Salesforce can initiate SLO. The Custom Logout URL must be an absolute URL and start with `http://` or `https://`.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Federated Authentication is available in: **All** Editions

Delegated Authentication is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Authentication Providers are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view the settings:

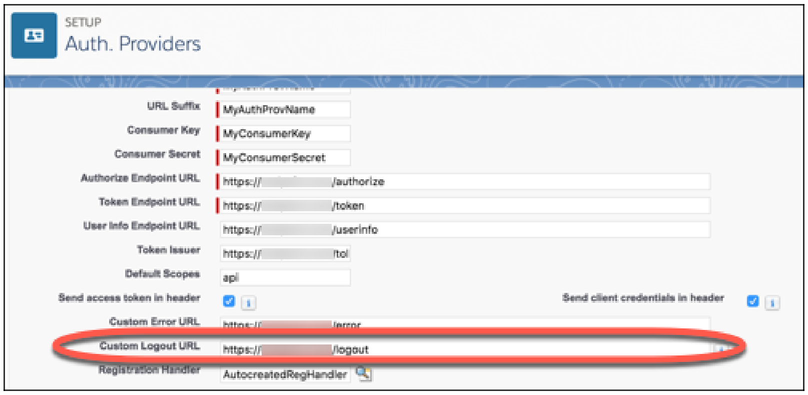
- View Setup and Configuration

To edit the settings:

- Customize Application

  AND

  Modify All Data



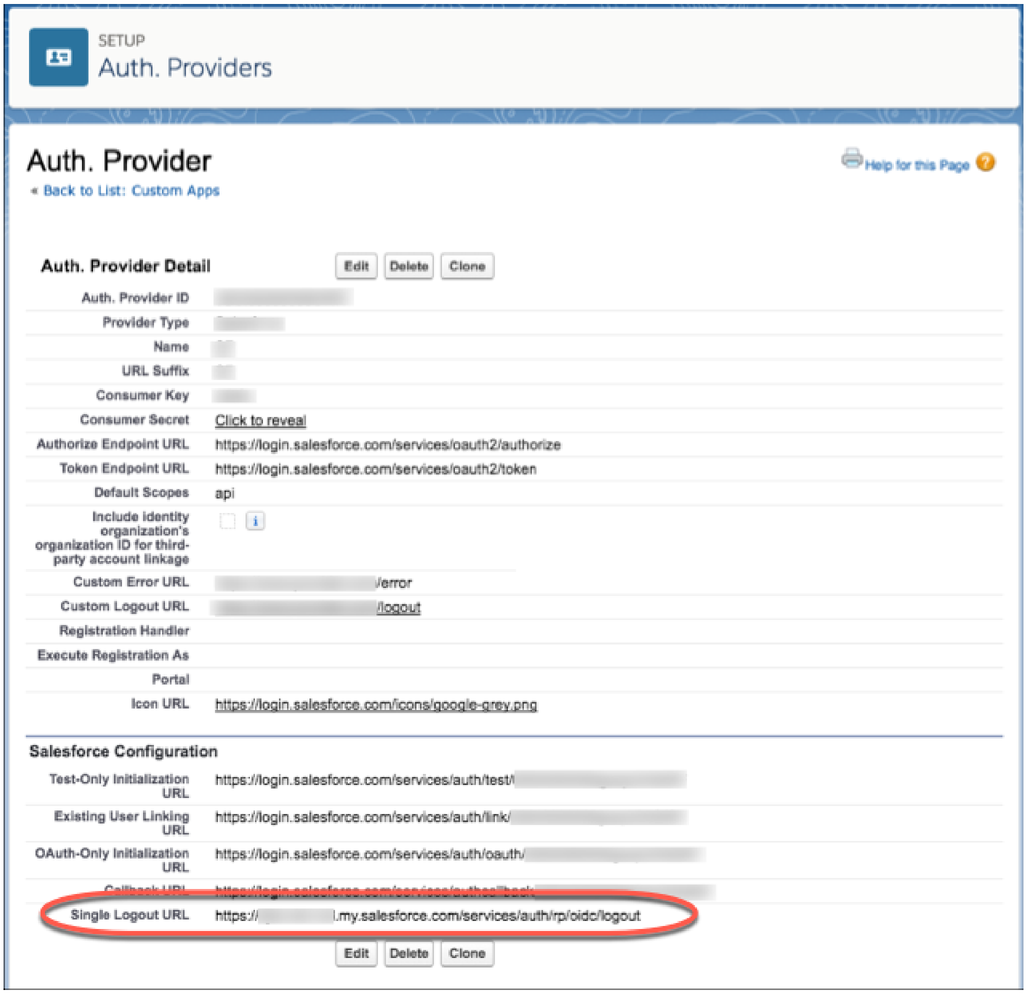
SETUP

Auth. Providers

URL Suffix	MyAuthProvName
Consumer Key	MyConsumerKey
Consumer Secret	MyConsumerSecret
Authorize Endpoint URL	https://[redacted]/authorize
Token Endpoint URL	https://[redacted]/token
User Info Endpoint URL	https://[redacted]/userinfo
Token Issuer	https://[redacted]/tol
Default Scopes	api
Send access token in header	☑
Send client credentials in header	☑
Custom Error URL	https://[redacted]/error
Custom Logout URL	https://[redacted]/logout
Registration Handler	AutocreatedRegHandler

4. Click **Save**.

5. Provide your authentication provider with the Salesforce SLO endpoint. With this endpoint, the authentication provider can initiate SLO. It's the **Single Logout URL** found under Salesforce Configuration on the Auth. Provider detail page. The format for the endpoint is `https://<domain>.my.salesforce.com/services/auth/rp/oidc/logout`, where `<domain>` is your org's My Domain name.



SETUP

Auth. Providers

Auth. Provider

« Back to List: Custom Apps

Help for this Page

Auth. Provider Detail [Edit] [Delete] [Clone]

Auth. Provider ID	[redacted]
Provider Type	[redacted]
Name	[redacted]
URL Suffix	[redacted]
Consumer Key	[redacted]
Consumer Secret	Click to reveal
Authorize Endpoint URL	https://login.salesforce.com/services/oauth2/authorize
Token Endpoint URL	https://login.salesforce.com/services/oauth2/token
Default Scopes	api
Include identity organization's organization ID for third-party account linkage	□
Custom Error URL	[redacted]/error
Custom Logout URL	[redacted]/logout
Registration Handler	
Execute Registration As	
Portal	
Icon URL	https://login.salesforce.com/icons/google-grey.png

Salesforce Configuration

Test-Only Initialization URL	https://login.salesforce.com/services/auth/test/[redacted]
Existing User Linking URL	https://login.salesforce.com/services/auth/link/[redacted]
OAuth-Only Initialization URL	https://login.salesforce.com/services/auth/oauth/[redacted]
Callback URL	https://login.salesforce.com/services/authcallback/[redacted]
Single Logout URL	https://[redacted].my.salesforce.com/services/auth/rp/oidc/logout

[Edit] [Delete] [Clone]

SEE ALSO:

Single Logout

External Authentication Providers

Configure OpenID Connect Settings for Single Logout Where Salesforce Is the OpenID Connect Provider

Configure SLO when Salesforce provides authentication for users to access a relying provider using OpenID Connect. Users log in to Salesforce. Salesforce uses OpenID Connect to authenticate users for the relying party through a connected app. When the users log out of the relying party (or Salesforce) session, they're automatically logged out of both.

To use this feature:

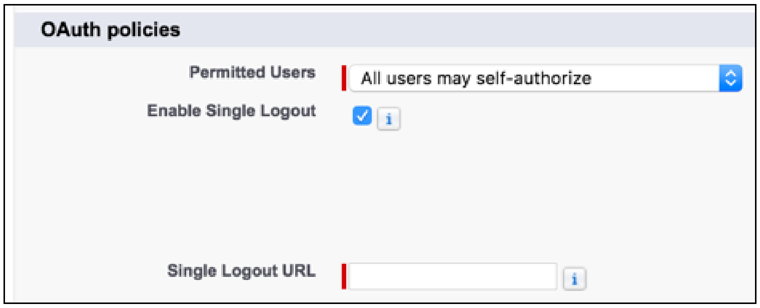
- Enable My Domain.
- Make sure the relying party supports OpenID Connect SLO.
- Get the OpenID Connect SLO logout endpoint from the relying party.

This implementation uses connected apps. You can configure SLO when you create and edit a connected app as a developer, and distribute it to other orgs. Or, you can create and manage SLO for a connected app within your org as an administrator. Changes to the SLO configuration in the connected app management page are not propagated back to the page when you're editing a connected app as a developer. As you change settings through connected app management pages, manually copy settings to the app creation page, if desired.

Also, after the initial creation of the connected app, changes to the SLO configuration for the connected app development page do not propagate to the administration page, automatically.

These steps edit an existing connected app. The fields are the same when you create, or manage, a connected app.

1. In Setup, enter `apps` in the `Quick Find` box, then select **Manage Connected Apps**.
2. Next to the connected app that you want to configure for SLO, click **Edit**.
3. Under **OAuth Policies**, select **Enable Single Logout**.



OAuth policies

Permitted Users: All users may self-authorize

Enable Single Logout: ☑

Single Logout URL:

4. For **Single Logout URL**, enter the OpenID Connect SLO endpoint of the connected app's relying party. This endpoint is where Salesforce sends a logout request when users log out of Salesforce. The relying party provides you with this endpoint. The Single Logout URL must be an absolute URL and start with `https://`.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Federated Authentication is available in: **All** Editions

Delegated Authentication is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Authentication Providers are available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To view the settings:

- View Setup and Configuration

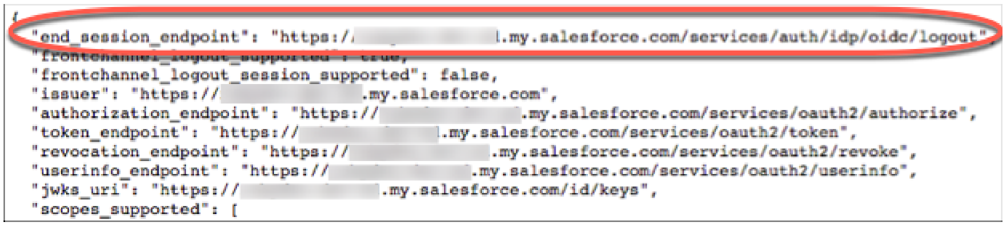
To edit the settings:

- Customize Application

  AND

  Modify All Data

5. Use the OpenID Connect Discovery Endpoint to provide your relying party with the Salesforce identity provider SLO endpoint. With this endpoint, the relying party can initiate SLO. It's found in *`https://<domain>.my.salesforce.com/.well-known/openid-configuration`*, where *`<domain>`* is your org's My Domain name. The format for the endpoint is *`https://<domain>.my.salesforce.com/services/auth/idp/oidc/logout`*, also where *`<domain>`* is your org's My Domain name.



```
{
  "end_session_endpoint": "https:/[redacted].my.salesforce.com/services/auth/idp/oidc/logout",
  "frontchannel_logout_supported": true,
  "frontchannel_logout_session_supported": false,
  "issuer": "https://[redacted].my.salesforce.com",
  "authorization_endpoint": "https://[redacted].my.salesforce.com/services/oauth2/authorize",
  "token_endpoint": "https://[redacted].my.salesforce.com/services/oauth2/token",
  "revocation_endpoint": "https://[redacted].my.salesforce.com/services/oauth2/revoke",
  "userinfo_endpoint": "https://[redacted].my.salesforce.com/services/oauth2/userinfo",
  "jwks_uri": "https://[redacted].my.salesforce.com/id/keys",
  "scopes_supported": [
```

SEE ALSO:

Single Logout

My Domain

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Add a subdomain to your Salesforce org URL with the My Domain Salesforce feature. Having a subdomain lets you highlight your brand and makes your org more secure. A subdomain is convenient and allows you to personalize your login page.

Using My Domain, you define a subdomain that's part of your Salesforce domain. For example, `developer` is a subdomain of the `salesforce.com` domain. With a subdomain, you replace the URL that Salesforce assigned you, like `https://na30.salesforce.com`, with your chosen name, like `https://somethingcool.my.salesforce.com`. A subdomain is also referred to as a custom domain. However, a custom domain has a specific meaning for Salesforce Communities.

A subdomain name helps you better manage login and authentication for your org in several key ways. You can:

- Highlight your business identity with your unique domain URL
- Brand your login screen and customize right-frame content
- Block or redirect page requests that don't use the new domain name
- Work in multiple Salesforce orgs at the same time
- Set custom login policy to determine how users are authenticated
- Let users log in using a social account, like Google and Facebook, from the login page
- Allow users to log in once to access external services

My Domain is required before you can use these Salesforce features:

- Single sign-on (SSO) with external identity providers
- Social sign-on with authentication providers, such as Google and Facebook
- Lightning components in Lightning component tabs, Lightning pages, the Lightning App Builder, or standalone apps

Watch a Demo (5:11 minutes)

My Domain is also available for sandbox environments.

Your domain name uses standard URL format, including:

- Protocol: https://
- Subdomain prefix: your brand or term
- Domain: my.salesforce.com

Your name can include up to 40 letters, numbers, and hyphens. You can't start the subdomain name with root, status, or a hyphen.

You have the chance to try out names and check availability before you commit to your domain name.

Salesforce is enabled as an identity provider when a domain is created. After your domain is deployed, you can add or change identity providers and increase security for your org by customizing your domain's login policy.

Important: After you deploy your domain, it's activated immediately, and requests with the original URL are redirected to your new domain. Only Salesforce Customer Support can change your domain name after it's deployed.

IN THIS SECTION:

Set Up a My Domain Name

Implementing your subdomain name with My Domain is quick and easy.

Define Your Domain Name

Register your org's custom domain name with My Domain. You can try out names and check availability before registering the name.

Guidelines and Best Practices for Implementing My Domain

These tips smooth the transition to using the subdomain that you created with My Domain.

Test and Deploy Your New My Domain Subdomain

After you set up your subdomain with My Domain, test it and then roll it out to your users. Testing gives you the chance to explore your subdomain. It also helps you verify URLs for pages before rolling out the subdomain to your users.

My Domain URL Changes

When you set up a subdomain name for your org with My Domain, all your application URLs, including Visualforce pages, also change. Make sure that you update all application URLs before you deploy a domain name. For example, the `Email Notification URL` field in Chatter Answers continues to send notifications with the old URLs to internal users unless you update it. This table shows you the differences.

Set the My Domain Login Policy

Manage your user logins by customizing the login policy for your domain. By default, users log in from a generic Salesforce login page, bypassing the login page specific to your domain. If you don't set a login policy, users can make page requests without your domain name, such as when using old bookmarks.

Customize Your My Domain Login Page with Your Brand

Customize the look and feel of your login page by changing the background color, logo, or right-side (iframe) content. Customizing your Salesforce login page with your company's branding helps users recognize your page.

Add Identity Providers on a Login Page

Allow users to authenticate using alternate identity provider options right from your login page. If you've enabled single sign-on and configured SAML, or set up external authentication providers as Auth. Providers in Setup, you can provide links to these identity providers on your domain's login page. Users are sent to the identity provider's login screen to authenticate and then redirected back to Salesforce.

Get System Performance and Maintenance Information with My Domain

You can get information about system performance and availability from `trust.salesforce.com`. Trust reports status information based on your org instance. If you're using My Domain and don't know your org instance, you can look it up.

My Domain FAQ

Set Up a My Domain Name

Implementing your subdomain name with My Domain is quick and easy.

1. Find a domain name that's available and sign up for it.
2. Customize the logo, background color, and right-frame content on your login page.
3. Add or change the identity providers available on your login page.
4. Test your domain name and deploy it to your entire org.
5. Set the login policy for users accessing your pages.

SEE ALSO:

My Domain

Define Your Domain Name

Test and Deploy Your New My Domain Subdomain

Set the My Domain Login Policy

Customize Your My Domain Login Page with Your Brand

Add Identity Providers on a Login Page

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To set up a domain name:
- Customize Application

Define Your Domain Name

Register your org's custom domain name with My Domain. You can try out names and check availability before registering the name.

Start setting up your My Domain subdomain by finding a domain name unique to your org and registering it. Choose your name carefully. When you register, Salesforce updates its domain name registries with your domain name. After the name is registered, only Salesforce Customer Support can disable or change your domain name.

1. From Setup, enter *`My Domain`* in the `Quick Find` box, then select **My Domain**.
2. Enter the subdomain name you want to use within the sample URL. For example, if a company called Universal Containers uses the subdomain `universalcontainers`, the company's login URL is `https://universalcontainers.my.salesforce.com/`. Your name can include up to 40 letters, numbers, and hyphens.

   You can't use these reserved words for subdomains:

   - www
   - salesforce
   - heroku

   You can't start the domain name with:

   - root
   - status
   - a hyphen (-)

3. Click **Check Availability**. If your name is already taken, choose a different one.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To define a domain name:
- Customize Application

4. Click **Register Domain**.
5. You receive an email when your domain name is ready for testing. It can take a few minutes.

The new subdomain is available to your users after you test and deploy it.

SEE ALSO:

Set Up a My Domain Name

Guidelines and Best Practices for Implementing My Domain

My Domain URL Changes

Test and Deploy Your New My Domain Subdomain

Guidelines and Best Practices for Implementing My Domain

These tips smooth the transition to using the subdomain that you created with My Domain.

- Communicate the upcoming change to your users before deploying it.
- Deploy your new subdomain when your org receives minimal traffic, like during a weekend, so you can troubleshoot while traffic is low.
- If you've customized your Salesforce UI with features, such as custom buttons or Visualforce pages, make sure that you test your customizations thoroughly before deploying your domain name. Look for broken links due to hard-coded references (instance-based URLs), and use your subdomain URLs instead. For more information, enter "hard-coded references" in *Salesforce Help* Test them in a sandbox environment first.
- Make sure that you update all application URLs before you deploy a domain name. For example, the `Email Notification URL` field in Chatter Answers continues to send notifications with the old URLs to internal users unless you update it.
- If your domain is registered but has not yet been deployed, URLs contain your subdomain name when you log in from the My Domain login page. However, links that originate from merge fields that are embedded in emails sent asynchronously, such as workflow emails, still use the old URLs. *After* your domain is deployed, those links show the new My Domain URLs.
- Help your users get started using your new subdomain by providing links to pages they use frequently, such as your login page. Let your users know if you changed the login policy, and encourage them to update their bookmarks the first time they're redirected.
- Choose the Redirect Policy option **Redirected with a warning to the same page within the domain** to give users time to update their bookmarks with the new subdomain name. After a few days or weeks, change the policy to **Not redirected**. This option requires users to use your subdomain name when viewing your pages. It provides the greatest level of security.
- Only use **Prevent login from https://login.salesforce.com** if you're concerned that users who aren't aware of your subdomain try to use it. Otherwise, leave the option available to your users while they get used to the new domain name.
- Bookmarks don't work when the **Redirect to the same page within the domain** option is selected for partner portals. Manually change the existing bookmarks to point to the new domain URL by replacing the Salesforce instance name with your custom domain name. For example, replace `https://na30.salesforce.com/` with `https://`*`yourDomain`*`.my.salesforce.com/` in the bookmark's URL.
- If you block application page requests that don't use the new Salesforce subdomain URLs, let your users know that they must either update old bookmarks or create new ones for the login page. They must also update tabs or links within the app. If you change your login redirect policy to **Not Redirected**, users must use the new subdomain URLs immediately.
- If you are using My Domain, you can identify which users are logging in with the new login URL and when. From Setup, enter *`Login History`* in the `Quick Find` box, then select **Login History** and view the Username and Login URL columns.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

- On the `login.salesforce.com` page, users can click **Log in to a custom domain** to enter your subdomain name and log in. In this case, they must know the subdomain name. As a safeguard, give them a direct link to your subdomain's login page as well.

If You Have the Following	Do the Following
API integrations into your org	Check to see if the API client is directly referencing the server endpoint. The API client should use the LoginResult.serverURL value returned by the login request, instead of using a hard-coded server URL. After your subdomain is deployed, Salesforce returns the server URL containing your domain. Redirect policy settings have no effect on API calls. That is, old calls to instance URLs continue to work. However, the best practice is to use the value returned by Salesforce.
Email templates	Replace references to the org's instance URL with your subdomain.
Custom Visualforce pages or custom Force.com apps	Replace references to the org's instance URL with your subdomain. See How to find hard-coded references with the Force.com IDE.
Chatter	Tell your users to update any bookmarks in the left navigation of their Chatter groups.
Zones for Communities (Ideas/Answers/Chatter Answers)	Manually update the email notification URL. To update the URL, clear the existing URL so that the field is blank and save the page. Then the system populates the field with your new My Domain URL.

SEE ALSO:

My Domain URL Changes

Test and Deploy Your New My Domain Subdomain

My Domain

Test and Deploy Your New My Domain Subdomain

After you set up your subdomain with My Domain, test it and then roll it out to your users. Testing gives you the chance to explore your subdomain. It also helps you verify URLs for pages before rolling out the subdomain to your users.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To set up a domain name:
- Customize Application

Important: After you deploy your domain, it's activated immediately, and requests with the original URL are redirected to your new domain. Only Salesforce Customer Support can change your domain name after it's deployed.

1. Test your domain login. From Setup, enter `My Domain` in the Quick Find box, then select **My Domain**. Or, log out of your DE org and log in to Salesforce using your new subdomain name. Or, click the login link in the activation email you received.

   You can customize your domain login page and add authentication services (like social sign-on) before you deploy the domain to your users. You can also test the domain in a sandbox environment.

2. Test the new domain name by clicking tabs and links. All pages now show your new domain name.

   If you've customized your Salesforce UI with features, such as custom buttons or Visualforce pages, make sure that you test your customizations thoroughly before deploying your domain name. Look for broken links due to hard-coded references (instance-based URLs), and use your subdomain URLs instead. For more information, enter "hard-coded references" in *Salesforce Help*

3. To roll out the new domain name to your org, from Setup, enter `My Domain` in the Quick Find box, then select **My Domain**. Click **Deploy to Users**, and click **OK**.

When you deploy your domain, it's activated immediately, and all users are redirected to pages with new domain addresses. You can now set login policies in the Domain Settings section that appears after you deploy your domain. For example, you can prevent users from logging in from login.salesforce.com.

SEE ALSO:

Set Up a My Domain Name

Guidelines and Best Practices for Implementing My Domain

Customize Your My Domain Login Page with Your Brand

Add Identity Providers on a Login Page

Set the My Domain Login Policy

My Domain URL Changes

When you set up a subdomain name for your org with My Domain, all your application URLs, including Visualforce pages, also change. Make sure that you update all application URLs before you deploy a domain name. For example, the `Email Notification URL` field in Chatter Answers continues to send notifications with the old URLs to internal users unless you update it. This table shows you the differences.

URL Type	Old URL	New URL
Login	`https://login.salesforce.com`	`https://<subdomain>.my.salesforce.com`
Application page or tab	`https://<instance>.salesforce.com/<pageID>`	`https://<subdomain>.my.salesforce.com/<pageID>`
Visualforce page with no namespace	`https://c.<instance>visual.force.com/apex/<pagename>`	`https://<subdomain>--c.<instance>.visual.force.com/apex/<pagename>`
Visualforce page *with* namespace	`https://<yournamespace101>.<instance>.visual.force.com/apex/<pagename>`	`https://<subdomain>--<yournamespace>.<instance>.visual.force.com/apex/`

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Note: If you implement My Domain in a sandbox environment, the URL format is `https://<subdomain>--<sandboxname>.<instance>.my.salesforce.com`. Because you can't have namespaces in a sandbox environment, the format of all Visualforce page URLs in a sandbox is `https://<subdomain>--<sandboxname>--c.<instance>.visual.force.com/apex/<pagename>`.

SEE ALSO:

My Domain

Guidelines and Best Practices for Implementing My Domain

Set the My Domain Login Policy

Manage your user logins by customizing the login policy for your domain. By default, users log in from a generic Salesforce login page, bypassing the login page specific to your domain. If you don't set a login policy, users can make page requests without your domain name, such as when using old bookmarks.

1. From Setup, enter `My Domain` in the `Quick Find` box, then select **My Domain**.
2. Under My Domain Settings, click **Edit**.
3. To disable authentication for users who don't use your domain-specific login page, set a login policy. Selecting the login policy prevents users from logging in on the generic `https://<instance>.salesforce.com/` login page and then being redirected to your pages after login.
4. Choose a redirect policy.
   a. To allow users to continue using URLs that don't include your domain name, select **Redirect to the same page within the domain**.

      Note: Bookmarks don't work when the **Redirect to the same page within the domain** option is selected for partner portals. Manually change the existing bookmarks to point to the new domain URL by replacing the Salesforce instance name with your custom domain name. For example, replace `https://na30.salesforce.com/` with `https://yourDomain.my.salesforce.com/` in the bookmark's URL.

   b. To remind users to use your domain name, select **Redirected with a warning to the same page within the domain**. After reading the warning, users are redirected to the page. Select this option for a few days or weeks to help users transition to a new domain name.
   c. To require users to use your domain name when viewing your pages, select **Not redirected**.
5. Click **Save**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To set login policy for a domain:
- Customize Application

SEE ALSO:

Set Up a My Domain Name

Guidelines and Best Practices for Implementing My Domain

Customize Your My Domain Login Page with Your Brand

Customize the look and feel of your login page by changing the background color, logo, or right-side (iframe) content. Customizing your Salesforce login page with your company's branding helps users recognize your page.

Setting Up a My Domain (5:10 minutes. Login page branding starts at 2:43.)

1. From Setup, enter `My Domain` in the Quick Find box, then select **My Domain**.
2. Under Authentication Configuration, click **Edit**.
3. To customize your logo, upload an image.

   Images can be .jpg, .gif, or .png files up to 100 KB. Maximum image size is 250px by 125px.
4. To customize your login page background, click the ▦ or enter a valid hexadecimal color code.
5. To support advanced authentication methods for iOS users, select **Use the native browser for user authentication on iOS**.

   This iOS user authentication option is for users of Salesforce and Mobile SDK applications on iOS devices. It enables support of authentication methods, such as Kerberos, Windows NT LAN Manager (NTLM), or certificate-based authentication. When you select this option, users on iOS devices are redirected to their native browser when using single sign-on authentication into your custom domain. For other operating systems, the Salesforce app and applications using Mobile SDK version 3.1 or later can support certificate-based authentication when the applications are integrated with Mobile Device Management (MDM) software.
6. Enter the URL of the file to be included in the right-side iframe on the login page.

   The content in the right-side iframe can resize to fill about 50% of the page. Your content must be hosted at a URL that uses SSL encryption and the https:// prefix. To build your own custom right-side iframe content page using responsive web design, use the My Domain Sample template.

   Example: `https://c.salesforce.com/login-messages/promos.html`
7. Optionally, select authentication services as identity providers on the login page, such as social sign-on providers like Google and Facebook. Users can then log in with their social account credentials. Configure authentication services as Auth. Providers in Setup.
8. Click **Save**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To customize a login page:

- Customize Application

SEE ALSO:

Set Up a My Domain Name

Add Identity Providers on a Login Page

Set the My Domain Login Policy

External Authentication Providers

Add Identity Providers on a Login Page

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To add identity providers on a login page:

- Customize Application

Allow users to authenticate using alternate identity provider options right from your login page. If you've enabled single sign-on and configured SAML, or set up external authentication providers as Auth. Providers in Setup, you can provide links to these identity providers on your domain's login page. Users are sent to the identity provider's login screen to authenticate and then redirected back to Salesforce.

Note: Available authentication services include all providers configured as SAML single sign-on identify providers or external authentication providers, except Janrain. You can't use Janrain for authentication from the login page.

1. From Setup, enter `My Domain` in the `Quick Find` box, then select **My Domain**.
2. Under Authentication Configuration, click **Edit**.
3. Select one or more already configured authentication services as an identity provider.
4. Click **Save**.

SEE ALSO:

Set Up a My Domain Name

Customize Your My Domain Login Page with Your Brand

Set the My Domain Login Policy

External Authentication Providers

Get System Performance and Maintenance Information with My Domain

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To set up a domain name:

- Customize Application

You can get information about system performance and availability from `trust.salesforce.com`. Trust reports status information based on your org instance. If you're using My Domain and don't know your org instance, you can look it up.

Here's how to get status information using your domain name.

1. Go to trust.salesforce.com.
2. Under System Status, click **Learn More**.
3. Under status.salesforce.com, click **Status**.

   The Status & Maintenance page shows the status for each org instance.
4. At the top right of the page, click **My Domain**.
5. Enter your domain name in the search bar to get your org instance.

   Don't enter the complete URL. For example, use `yourDomain`, not `https://yourDomain.my.salesforce.com/`.
6. Under Status & Maintenance, select **All**, and look for your instance.

SEE ALSO:

My Domain

My Domain FAQ

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Performance**, **Unlimited**, **Enterprise**, **Developer**, and **Database.com** Editions. Some topics don't apply to **Database.com**.

IN THIS SECTION:

What is My Domain?

Using My Domain, Salesforce admins can define a subdomain within their Salesforce org. The subdomain name appears in all org URLs and replaces the instance name (such as na30). For example, you can brand your URL by naming the subdomain your company name, `https://`*`myCompanyName`*`.my.salesforce.com/`. My Domain is not the same as the custom domain for sites, communities, or portals. The domains are defined separately.

Which Salesforce Editions is My Domain available in?

Performance, Unlimited, Enterprise, Developer, Professional, and Group editions.

What are the advantages of My Domain?

Create a subdomain with My Domain to enable users to single sign-on into your org. You can also customize your login page and use Salesforce as an identity provider.

My Domain allows you to:

- Customize the login page with your own branding.

- Use Identity features for single sign-on. My Domain is required to:
  - Enable users to single sign-on into a Salesforce org
  - Use a Salesforce org as an identity provider for single sign-on into third-party applications or other Salesforce orgs
- Preserve deep links (such as `https://`*`yourDomain`*`.my.salesforce.com//001/o`) through any future org splits and migrations.

Does My Domain work differently in different Salesforce Editions?

My Domain works the same in most Salesforce editions except for Developer Edition URLs. Developer Edition URLs end with "-de-ed.my.salesforce.com", for example, `https://`*`yourDomain`*`.de-ed.my.salesforce.com`. URLs in other editions end with ".my.salesforce.com", for example, `https://`*`yourDomain`*`.my.salesforce.com`.

Does My Domain work in sandboxes?

Sandboxes and production orgs are different environments and maintain separate domain name registries. So you can use the same My Domain name in sandbox. In fact, during a sandbox refresh, the My Domain name of the production org is copied into sandbox.

For example, if the production org name is `acme.my.saleforce.com`, the sandbox name is `acme--<sandboxName>.csN.my.salesforce.com`.

Test your subdomain in sandbox before deploying it. Look for hard-coded references to instance URLs in Visualforce pages, email templates, and other content.

What are the differences between the redirect policy options?

After you deploy your subdomain with My Domain, you can select a redirect option for users trying to access a page in your org without using your subdomain name.

To see the assigned policy, from Setup, enter *`My Domain`* in the `Quick Find` box, then select **My Domain**.

If **Redirected to the same page within the domain** is selected, users are immediately sent to the new URL, without notification.

If **Redirected with a warning to the same page within the domain** is selected, users briefly see a warning message before being redirected to the new URL. The warning gives users a chance to change their bookmarks and get used to using the new subdomain URL. You can't customize the message.

If **Not redirected** is selected, the user gets a "page not found" error. Eventually, you want your users to use only subdomain URLs, but it's a best practice to use **Redirected with a warning to the same page within the domain** for a short time after you deploy your subdomain so that users can get used to the new URLs.

How does My Domain work with single sign-on?

My Domain is required for setting up single sign-on. For inbound single sign-on requests, the subdomain enables deep linking directly to pages in the org. No changes are required for the identity provider. The Salesforce SAML endpoint (`login.salesforce.com`) continues to work for SAML and OAUTH requests, even if your org deploys My Domain and selects **Prevent login from https://login.salesforce.com** in the My Domain Settings.

Note: If you're using external Chatter groups along with single sign-on for employees, users outside your company are redirected to a SAML identity provider that they can't access. To get single sign-on to work, migrate external Chatter groups to communities. Or, from the My Domain settings, do *not* select `Prevent login from https://login.salesforce.com`. Doing so allows users to continue to log in through `login.salesforce.com`.

Is My Domain available for the API?

Yes, you can use the Salesforce APIs with your My Domain subdomain.

Is the subdomain for My Domain related to the subdomain for Sites or Communities?

No. The subdomain names you use for Sites and My Domain can be the same or different. We like to refer to Sites and Salesforce Communities as custom domains and My Domain as subdomains.

How long can the subdomain name be?

Your subdomain name can be up to 40 characters. The protocol (`https://`) and the domain (`my.salesforce.com`) are not included in the limit.

After we set up My Domain, will we still be able to log in from **`https://login.salesforce.com`**?

Yes, unless your system administrator prevents it. If so, you'll need to log in using your new My Domain URL.

Will we still be able to log in from a URL that includes a Salesforce instance, like **`https://`***`yourInstance`***`.salesforce.com/`**?

Yes, unless your system administrator prevents it. If so, you'll need to log in using your new My Domain URL.

Can we still use our old Salesforce bookmarks?

Yes, if your system administrator allows it. If so, you'll be redirected to the Salesforce page using its new My Domain URL. If your system administrator prevents using old bookmarks, or you see a warning, you should update your bookmarks using the new domain name.

Will our Visualforce and content (files) page URLs change?

URLs for your Visualforce pages contain your new domain name, such as `https://<mydomain>--c.<instance>.visual.force.com`.

URLs for your content (files) also contain your new domain name, such as `https://<mydomain>--c.<instance>.content.force.com`.

Can I change or remove my subdomain name?

You can’t change the subdomain name that you create with My Domain. And after your subdomain is deployed, you can’t reverse deployment. If you need to change your subdomain name, contact Salesforce Customer Support.

App Launcher

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

The App Launcher is how users switch between apps. It displays tiles that link to a user's available Salesforce, connected (third-party), and on-premises apps. You can determine which apps are available to which users and the order in which the apps appear. You can also make the App Launcher the default landing page when users first open Salesforce.

The App Launcher is available to all Lightning Experience and Salesforce Classic users. Salesforce Classic users need the Use Identity Features permission and the App Launcher option in their profile set to **Visible**. Users see only the apps that they are authorized to see according to their profile or permission sets.

In Salesforce Classic, Salesforce admins using the System Administrator profile have access to the App Launcher. Admins using profiles cloned from the System Administrator profile don't.

IN THIS SECTION:

Enable the App Launcher with a Profile in Salesforce Classic
Create a profile and assign it to users, so they can access the App Launcher.

Enable the App Launcher with a Permission Set in Salesforce Classic
Create a permission set and assign it to users, so they can access the App Launcher.

SEE ALSO:

Access Other Salesforce Apps
Set the Default Sort Order for Apps
Connected Apps
Identity Implementation Guide

Enable the App Launcher with a Profile in Salesforce Classic

EDITIONS

Available in: Salesforce Classic

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

Create a profile and assign it to users, so they can access the App Launcher.

Note: These steps work in Salesforce Classic. If you see the App Launcher icon (⁝⁝⁝) on the left side of the navigation bar at the top of your screen, you're in Lightning Experience. If not, you're in Salesforce Classic.

In Salesforce Classic, Salesforce admins using the System Administrator profile have access to the App Launcher. Admins using profiles cloned from the System Administrator profile don't.

1. From Setup, enter *Profiles* in the `Quick Find` box, then select **Profiles**.
2. Click **New Profile**.
3. Select an Existing Profile as a basis for the new profile.

   For example, select **Standard User**.
4. Enter the name of the new profile.

   For example, *Standard User Identity*.
5. Click **Save**.
6. In the detail page for the new profile, click **Edit**.
7. In Custom App Settings, set the App Launcher to **Visible**, if it isn't already.

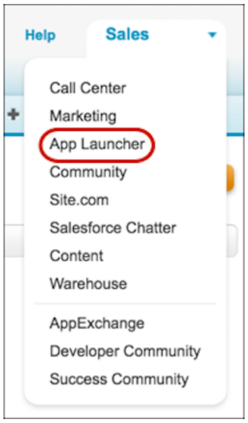
Under Tab Settings, verify that the App Launcher tab is set to `Default On`.

8. Under Administrative Permissions, select **Use Identity Features**.
9. Click **Save**.
10. From Setup, enter *`Users`* in the `Quick Find` box, then select **Users**.
11. Click **Edit** next to each user you want to access the App Launcher.
12. In the user's Profile field, select the new profile that has "Use Identity Features" enabled.

    For example, you might use the *`Standard User Identity`* profile.

13. Click **Save**.

    When you log in as the selected user, the App Launcher appears in the drop-down app menu.



SEE ALSO:

App Launcher

Enable the App Launcher with a Permission Set in Salesforce Classic

Create a permission set and assign it to users, so they can access the App Launcher.

EDITIONS

Available in: Salesforce Classic

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

Note: These steps work in Salesforce Classic. If you see the App Launcher icon (⠿) on the left side of the navigation bar at the top of your screen, you're in Lightning Experience. If not, you're in Salesforce Classic.

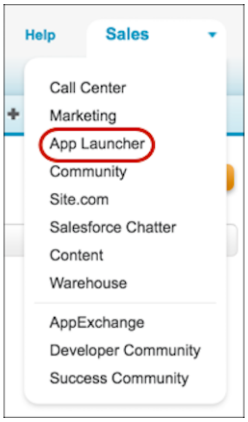
1. From Setup, enter *`Permission Sets`* in the `Quick Find` box, then select **Permission Sets**.
2. Click **New**.
3. Enter a Label for the new permission set.

   For example, *`Identity Features`*.

4. Optionally, restrict the use of this permission set to a specific User License.
5. Click **Save**.
6. Click **System Permissions**.

7. Click **Edit**.
8. Select **Use Identity Features**.
9. Click **Save**.
10. From Setup, enter *`Users`* in the `Quick Find` box, then select **Users**.
11. Click the name of an existing user to whom you want to give access to the App Launcher.
12. In the **Permission Set Assignments** related list, click **Edit Assignments**.
13. Add the new permission set you created for identity features to Enabled Permission Sets.
14. Click **Save**.

    When you log in as the selected user, the App Launcher appears in the drop-down app menu.



Note: Still not seeing the App Launcher? In the profile associated with the user, select **Visible** for the App Launcher setting.

SEE ALSO:

App Launcher

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`.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

USER PERMISSIONS

To configure file upload and download settings:

- Customize Application

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**.

Certificates and Keys

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To create, edit, and manage certificates:
- Customize Application

Salesforce certificates and key pairs are used for signatures that verify a request is coming from your organization. They are used for authenticated SSL communications with an external web site, or when using your organization as an Identity Provider. You only need to generate a Salesforce certificate and key pair if you're working with an external website that wants verification that a request is coming from a Salesforce organization.

You can export all your certificates and private keys into a keystore for storage or import certificates and keys from a keystore. This allows you to move keys from one organization to another. The exported file is in the Java Keystore (JKS) format, and the imported file must also be in the JKS format. For more information about the JKS format, see Oracle's Java KeyStore documentation.

API Client Certificate

The API client certificate is used by workflow outbound messages, the AJAX proxy, and delegated authentication HTTPS callouts. For security reasons, the API client certificate should be known only to your org.

Choose an API client certificate based on the remote endpoint you connect to. Some endpoint servers require a certificate chain that is trusted by a certificate authority; others are fine with directly trusting a self-signed certificate.

IN THIS SECTION:

Generate a Self-Signed Certificate

Generate a certificate signed by Salesforce to show that communications purporting to come from your organization are really coming from there.

Generate a Certificate Signed by a Certificate Authority

A certificate authority-signed (CA-signed) certificate can be a more authoritative way to prove that your org’s data communications are genuine. You can generate this type of certificate and upload it to Salesforce.

Set Up a Mutual Authentication Certificate

To prevent security from being compromised by simple impersonation, you can require clients and servers to prove their identity to each other with a mutual authentication certificate.

Configure Your API Client to Use Mutual Authentication

Enforce SSL/TLS mutual authentication.

Manage Master Encryption Keys

Encrypted custom fields, such as `Social Security Number` or `Credit Card Number`, are encrypted with a master encryption key. This key is automatically assigned when you select fields to encrypt. You manage your own master key according to your organization's security and regulatory needs.

Replace the Default Proxy Certificate for SAML Single Sign-On

The proxy.salesforce.com default certificate has been retired due to its expiration and for security best practices. If your Salesforce org uses this certificate for SAML single sign-on, act now to prevent a possible interruption of service.

Generate a Self-Signed Certificate

Generate a certificate signed by Salesforce to show that communications purporting to come from your organization are really coming from there.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To create, edit, and manage certificates:

- Customize Application

1. From Setup, search for *`Certificate and Key Management`* in the `Quick Find` box.
2. Select **Create Self-Signed Certificate**.
3. Enter a descriptive label for the Salesforce certificate.

   This name is used primarily by administrators when viewing certificates.
4. Enter a unique name. You can use the name that's automatically populated based on the certificate label you enter.

   This name can contain only underscores and alphanumeric characters, and must be unique in your org. It must begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores. Use the unique name when referring to the certificate using the Force.com web services API or Apex.
5. Select a key size for your generated certificate and keys.

   Certificates with 2048-bit keys last one year and are faster than certificates with 4096-bit keys. Certificates with 4096-bit keys last two years.

   Note: After you save a Salesforce certificate, you can't change its type or key size.
6. Click **Save**.

   Downloaded self-signed certificates have `.crt` extensions.

   After you successfully save a Salesforce certificate, the certificate and corresponding keys are automatically generated.

You can have a maximum of 50 certificates.

SEE ALSO:

Certificates and Keys

Generate a Certificate Signed by a Certificate Authority

Generate a Certificate Signed by a Certificate Authority

A certificate authority-signed (CA-signed) certificate can be a more authoritative way to prove that your org's data communications are genuine. You can generate this type of certificate and upload it to Salesforce.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To create, edit, and manage certificates:

- Customize Application

1. From Setup, enter `Certificate and Key Management` in the `Quick Find` box, then select **Certificate and Key Management**.
2. Select **Create CA-Signed Certificate**.
3. Enter a descriptive label for the Salesforce certificate.

   This name is used primarily by administrators when viewing certificates.
4. Enter a unique name. You can accept the name that's populated based on the certificate label you enter.

   This name can contain only underscores and alphanumeric characters, and must be unique in your org. It must begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores. Use the unique name when referring to the certificate using the Force.com web services API or Apex.
5. Select a key size for your certificate and keys.

   We recommend that you use the default key size of 2048 for security reasons. Selecting **2048** generates a certificate using 2048-bit keys. Selecting **4096** generates a certificate using 4096-bit keys.

   Note: After you save a Salesforce certificate, you can't change its type or key size.
6. Enter the following information.

   These fields are combined to generate a unique certificate.

Field	Description
`Common Name`	The fully qualified domain name of the company requesting the signed certificate, generally of the form `http://www.mycompany.com`.
`Email Address`	The email address associated with this certificate.
`Company`	Either the legal name of your company or your legal name.
`Department`	The branch of your company using the certificate, such as marketing or accounting.
`City`	The city where the company resides.
`State`	The state where the company resides.
`Country Code`	A two-letter code indicating the country where the company resides. For the United States, the value is *US*.

7. Click **Save**.

   After you save a Salesforce certificate, the certificate and corresponding keys are automatically generated.
8. Find your new certificate from the certificates list, then click **Download Certificate Signing Request**.

   Downloaded certificate signing requests have `.csr` extensions.

9. Send the certificate request to the certificate authority of your choice.
10. After the certificate authority sends back the signed certificate, go back to `Certificate and Key Management`, click the name of the certificate, then click **Upload Signed Certificate**.

    The CA-signed certificate must match the certificate created in Salesforce. If you try to upload a different CA-signed certificate, the upload fails.
11. To complete the upload process, click **Save**.

After you upload the CA-signed certificate, the status of the certificate is changed to Active and you can use it.

Tip: If you need to edit a certificate that you've uploaded, upload it again; Published site domains are republished if they have at least one Force.com site or community. The expiration date of the certificate record is updated to the expiration date of the newly uploaded certificate.

You can have up to 50 certificates.

Set Up a Mutual Authentication Certificate

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create, edit, and manage certificates:

- Customize Application

To prevent security from being compromised by simple impersonation, you can require clients and servers to prove their identity to each other with a mutual authentication certificate.

1. On the Certificate and Key Management page, click **Upload Mutual Authentication Certificate**.

    Note: If you don't see this option on the Certificate and Key Management page, contact Salesforce to enable the feature.
2. Give your certificate a label and name and click **Choose File** to locate the certificate.
3. Click **Save** to finish the upload process.
4. Enable the "Enforce SSL/TLS Mutual Authentication" user permission for an "API Only" user.

    This "API Only" user configures the API client to connect on port 8443 to present the signed client certificate.

If you are using a certificate chain, the client certificate must include any intermediate certificates in the chain when contacting port 8443.

A certificate chain is a hierarchical order of certificates where one certificate issues and signs another certificate lower in the hierarchy. Upload a certificate chain as a single PEM-encoded CA-signed certificate representing the concatenated chain of certificates. The uploaded certificate chain must include the intermediate certificates in the following order.

- Start with the server or client certificate and then add its signing certificate.
- If more than one intermediate certificate exists between the server or client certificate and the root, add each certificate as the one that signed the previous certificate.
- The root certificate is optional, and generally should not be included.

SEE ALSO:

Configure Your API Client to Use Mutual Authentication

Configure Your API Client to Use Mutual Authentication

Enforce SSL/TLS mutual authentication.

1. After you've set up mutual authentication, log in to the Salesforce service using port 8443. Include your credentials and your signed certificate information.
   For example, your configuration using `cURL` may look something like this, where "@login.txt" contains the login Soap message with your credentials and "fullcert.pem:xxxxxx" is your certificate information:

   ```
   curl -k https://login.salesforce.com:8443/services/Soap/u/31.0 -H "Content-Type: text/xml;
    charset=UTF-8" -H "SOAPAction: login" -d @login.txt -v -E fullcert.pem:xxxxxx
   ```

2. Once a session ID is returned from your call, you can perform other actions, such as queries. For example:

   ```
   curl -k https://yourInstance.salesforce.com:8443/services/Soap/u/31.0 -H "Content-Type:
    text/xml; charset=UTF-8" -H "SOAPAction: example" -d @accountQuery.xml -v -E
   fullcert.pem:xxxxxx
   ```

   where @accountQuery.xml is the file name containing the query Soap message with session ID from the login response.

SEE ALSO:

Certificates and Keys

Set Up a Mutual Authentication Certificate

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create, edit, and manage certificates:

- Customize Application

To Enforce mutual authentication on port 8443 for standard SSL/TLS connections:

(Assign to users with the Api Only User permission.)

- Enforce SSL/TLS Mutual Authentication

To access Salesforce only through a Salesforce API:

- Api Only User

Manage Master Encryption Keys

Encrypted custom fields, such as `Social Security Number` or `Credit Card Number`, are encrypted with a master encryption key. This key is automatically assigned when you select fields to encrypt. You manage your own master key according to your organization's security and regulatory needs.

With master encryption keys, you can:

- Archive the existing key and create a new key.
- Export an existing key after it's been archived.
- Delete an existing key.
- Import an existing key after it's been deleted.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To create, edit, and manage certificates:

- Customize Application

Archiving and Creating New Keys

To archive your current key and create a new key , click **Archive Current Key and Create New Key** on the *`Certificate and Key Management`* Setup page. A new key is generated, assigned the next sequential number, and activated. All new data is encrypted using the new key.

Existing data continues to use the archived key until the data is modified and saved. Then data is encrypted using the new key.

After you archive a key, you can export or delete it.

Exporting Keys

You can export your keys to a back-up location for safe keeping. It's a good idea to export a copy of any key before deleting it.

Exporting creates a text file with the encrypted key, so you can import the key back into your organization later.

Deleting Keys

Don't delete a key unless you're absolutely certain no data is currently encrypted using the key. After you delete a key, any data encrypted with that key can no longer be accessed.

Important: Export and delete keys with care. If your key is destroyed, you must reimport it to access your data. You are solely responsible for making sure your data and keys are backed up and stored in a safe place. Salesforce cannot help you with deleted, destroyed or misplaced keys.

Importing Keys

If you have data associated with a deleted key, you can import an exported key back into your organization. Any data that was not accessible becomes accessible again.

Click `Import` next to the key you want to import.

Note: This page is about Classic Encryption, not Shield Platform Encryption. What's the difference? on page 540

SEE ALSO:

Certificates and Keys

Replace the Default Proxy Certificate for SAML Single Sign-On

The proxy.salesforce.com default certificate has been retired due to its expiration and for security best practices. If your Salesforce org uses this certificate for SAML single sign-on, act now to prevent a possible interruption of service.

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

Beginning with the Winter '18 release, Salesforce is switching away from the default proxy certificate even if you are still using it. Before the Winter '18 release, manually migrate to a self-signed certificate and update identity providers to prevent an interruption in service. We recommend switching from the default certificate even if your identity provider doesn't validate signatures in SAML requests.

1. If you are using Single SAML Configurations, enable multiple configurations by clicking **Enable Multiple Configs** under Single Sign-On Settings. Read and understand all the instructions on that page. Enabling multiple configurations switches the certificate, so skip Step 2.
2. Edit each affected configuration by changing the Request Signing Certificate to a certificate in your org. If you don't have a certificate and key pair you want to use, upload one or select **Generate self-signed certificate**.
3. Check whether service provider-initiated SAML works properly for your configuration. If it does, no identity provider updates are necessary, and you can skip steps four and five.
   If you migrated from a single to multiple configurations, update the Assertion Consumer Service URL.
4. If identity provider updates are necessary, download the certificate you selected for the Request Signing Certificate.
5. Upload this certificate into the identity provider for use in validating SAML requests from Salesforce. If you migrated to multiple configurations from a single configuration, note the Salesforce Login URL and update the value in the identity provider.

SEE ALSO:

Certificates and Keys

Configure SAML Settings for Single Sign-On

Monitor Your Organization

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

IN THIS SECTION:

The System Overview Page

The system overview page shows usage data and limits for your organization, and displays messages when you reach 95% of your limit (75% of portal roles).

Monitor Data and Storage Resources

View your Salesforce org's storage limits and usage from the Storage Usage page in Setup.

Monitor Login History

Admins can monitor all login attempts for their org and enabled portals or communities. The login history page displays the most recent 20,000 attempts. To see more records, download the information to a CSV or GZIP file.

Identity Verification History

As an admin, use Identity Verification History to monitor and audit up to 20,000 records of your org users' identity verification attempts from the past six months. For example, suppose that two-factor authentication is enabled when a user logs in. When the user successfully provides a time-based, one-time password as proof of identity, that information is recorded in Identity Verification History.

Monitor Login Activity with Login Forensics

Login forensics helps administrators better determine which user behavior is legitimate to prevent identity fraud in Salesforce.

Monitor Training History

As an administrator, you want to know that your team is learning how to use Salesforce effectively. The Training Class History shows you all of the Salesforce training classes your users have taken.

Monitor Setup Changes

Setup Audit Trail tracks the recent setup changes that you and other admins have made to your org. Audit history is especially useful in orgs with multiple admins.

Field History Tracking

You can select certain fields to track and display the field history in the History related list of an object. The field history data is retained for up to 18 months.

Monitor Debug Logs

Set trace flags to trigger logging for users, Apex classes, and Apex triggers in the Developer Console or in Setup. Monitor the resulting logs to diagnose problems in your org.

Monitoring Scheduled Jobs

The All Scheduled Jobs page lists all reporting snapshots, scheduled Apex jobs, and dashboards scheduled to refresh.

Monitoring Background Jobs

You can monitor background jobs in your organization, such as when parallel sharing recalculation is running.

The System Overview Page

The system overview page shows usage data and limits for your organization, and displays messages when you reach 95% of your limit (75% of portal roles).

Note: The system overview page shows only the items enabled for your organization. For example, your system overview page shows workflow rules only if workflow is enabled for your organization.

Click the numbers under each metric to get more details about your usage. If it's available, use Checkout to increase usage limits for your organization. For example, if your organization reaches the limit for custom objects, the system overview page notifies you with a message link. Click the link to clean up any unused objects, or visit Checkout to increase your limit for objects.

To access the system overview page, from Setup, enter `System Overview` in the `Quick Find` box, then select **System Overview**.

The system overview page displays usage for:

- Schema
- API usage
- Business logic
- User interface
- Most used licenses

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: All Editions except **Personal** Edition

USER PERMISSIONS

To access the system overview page:

- Customize Application

- Portal roles

Note: The object limit percentages are truncated, not rounded. For example, if your org uses 95.55% of the limit for a particular customization, the object limit displays 95%.

IN THIS SECTION:

System Overview: Schema

The Schema box in the system overview page shows usage information for:

- Custom objects

  Note: Soft-deleted custom objects and their data count against your limits. We recommend that you hard delete or erase custom objects you no longer need.

- Data storage

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: All Editions except **Personal** Edition

System Overview: API Usage

The API Usage box in the system overview page shows usage information for API requests in the last 24 hours.

Limits are enforced against the aggregate of all API calls made by the org in a 24 hour period. Limits are not on a per-user basis. When an org exceeds a limit, all users in the org can be temporarily blocked from making additional calls. Calls are blocked until usage for the preceding 24 hours drops below the limit.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

System Overview: Business Logic

The Business Logic box in the system overview page shows usage information for:

- Rules
- Apex triggers
- Apex classes
- Code used: Total number of characters in your Apex triggers and Apex classes (excluding comments, test methods, and @isTest annotated classes).

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

System Overview: User Interface

The User Interface box in the system overview page shows usage information for:

- Custom apps
- Site.com sites: We only count published Site.com sites.
- Active Force.com sites
- Flows: We only count active flows.
- Custom tabs
- Visualforce pages

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

System Overview: Most Used Licenses

The Most Used Licenses box in the system overview page counts only active licenses, and by default shows the top three used licenses for your organization. Any license that reaches 95% usage also appears. Click **Show All** to view all the licenses for your organization.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: All Editions except **Personal** Edition

System Overview: Portal Roles

The Portal Roles box in the system overview page shows the usage data and limit for total partner portal, Customer Portal, and Communities roles. The system overview page displays a message when your organization reaches 75% of its allotted portal roles.

Note: The maximum number of roles used in an org's portals or communities is 5000. This limit includes roles associated with all of the organization's customer portals, partner portals, or communities. To prevent unnecessary growth of this number, we recommend reviewing and reducing the number of roles. You can also delete unused roles. If you require more roles, please contact Salesforce Customer Support.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Monitor Data and Storage Resources

View your Salesforce org's storage limits and usage from the Storage Usage page in Setup.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To view storage usage:

- Manage Internal Users

  AND

  Manage Users

Items That Require Storage

Storage is divided into two categories. File storage includes files in attachments, Files home, Salesforce CRM Content, Chatter files (including user photos), the Documents tab, the custom File field on Knowledge articles, and Site.com assets. Data storage includes the following:

- Accounts
- Article types (format: "[`Article Type Name`]")
- Article type translations (format: "[`Article Type Name`] Version")
- Campaigns
- Campaign Members
- Cases
- Case Teams
- Contacts
- Contracts
- Custom objects
- Email messages
- Events
- Forecast items
- Google docs
- Ideas
- Leads
- List Email
- Notes
- Opportunities
- Opportunity Splits
- Orders
- Quotes
- Quote Template Rich Text Data
- Solutions
- Tags: Unique tags
- Tasks

Storage Capacity

Data Storage

For data storage, Contact Manager, Group, Professional, Enterprise, Performance, and Unlimited Editions are allocated the greater of 1 GB or a per-user limit. For example, a Professional Edition org with 10 users receives 1 GB, because 10 users multiplied by 20 MB per user is 200 MB, which is less than the 1 GB minimum. A Professional Edition org with 100 users receives more than the 1 GB minimum, because 100 users multiplied by 20 MB per user is 2,000 MB.

File Storage

Contact Manager, Group, Professional, Enterprise, Performance, and Unlimited Editions are allocated 10 GB of file storage per org.

Orgs are allocated more file storage based on the number of standard user licenses. In Enterprise, Performance, and Unlimited Editions, orgs are allocated 2 GB of file storage per user license. Contact Manager, Group, Professional Edition orgs are allocated 612 MB per standard user license, which includes 100 MB per user license plus 512 MB per license for the Salesforce CRM Content feature license.

Note: Each Salesforce CRM Content feature license provides an extra 512 MB of file storage, whether Salesforce CRM Content is enabled or not.

The values in the File Storage Allocation Per User License column apply to Salesforce and Salesforce Platform user licenses.

Salesforce Edition	Data Storage Minimum per Org	Data Storage Allocation per User License	File Storage Allocation per Org	File Storage Allocation per User License
Contact Manager	1 GB	20 MB	10 GB	612 MB
Group				
Professional				
Enterprise				2 GB
Performance		120 MB		
Unlimited				
Developer	5 MB	N/A	20 MB	N/A
Personal	20 MB (approximately 10,000 records)			

If your org uses custom user licenses, contact Salesforce to determine if these licenses provide more storage. For a description of user licenses, see User Licenses.

Viewing Storage Usage

To view your org's current storage usage from Setup, enter `Storage Usage` in the `Quick Find` box, then select **Storage Usage**. You can view the available space for data storage and file storage, the amount of storage in use per record type, the top users according to storage utilization, and the largest files in order of size. To view what types of data a particular user is storing, click that user's name.

In all Editions except Personal Edition, administrators can view storage usage on a user-by-user basis.

1. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.
2. Click the name of any user.
3. Click **View** next to the `Used Data Space` or `Used File Space` fields to view that user's storage usage by record type.

Data storage and file storage are calculated asynchronously and your org's storage usage isn't updated immediately. Keep this in mind if importing or adding many records or files.

Individual users can view their own storage usage in their personal information.

Increasing Storage

When you need more storage, increase your storage limit or reduce your storage usage.

- Purchase more storage space, or add user licenses in Professional, Enterprise, Unlimited, and Performance Editions.
- Delete outdated leads or contacts.
- Remove any unnecessary attachments.
- Delete files in Salesforce CRM Content.

Storage Considerations

When planning your storage needs, keep in mind:

- Person accounts count against both account and contact storage because each person account consists of one account as well as one contact.
- Archived activities count against storage.
- Active or archived products, price books, price book entries, and assets don't count against storage.

Monitor Login History

Admins can monitor all login attempts for their org and enabled portals or communities. The login history page displays the most recent 20,000 attempts. To see more records, download the information to a CSV or GZIP file.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To monitor logins:

- Manage Users

Download Login History

You can download the past six months or the first 20,000 attempts of user logins to your Salesforce org to a CSV or GZIP file.

1. From Setup, enter *`Login History`* in the `Quick Find` box, then select **Login History**.
2. Select the file format to download.
   - **Excel csv file**—Download a CSV file of all user logins for the past six months or the first 20,000 user login attempts. This report includes logins through the API.
   - **gzipped Excel csv file**—Download a CSV file of all user logins for the past six months or the first 20,000 user login attempts. This report includes logins through the API. Because the file is compressed, it's the preferred option for quickest download time.
3. Select the file contents. The All Logins option includes API access logins.
4. Click **Download Now**.

Note: Older versions of Microsoft Excel can't open files with more than 65,536 rows. If you can't open a large file in Excel, see the Microsoft Help and Support article about handling large files.

Create List Views

You can create list views sorted by login time and login URL. For example, you can create a view of all logins between a particular time range. Like the default view, a custom view displays the most recent 20,000 logins.

1. On the Login History page, click **Create New View**.

2. Enter the name to appear in the View dropdown list.
3. Specify the filter criteria.
4. Select the fields to display.

   You can choose up to 15 fields. You can display only the fields that are available in your page layout. Text area fields display up to 255 characters.

   Note: Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.

View Your Login History

You can view your personal login history.

1. From your personal settings, enter *`Login History`* in the `Quick Find` box, then select **Login History**. No results? Enter *`Personal Information`* in the `Quick Find` box, then select **Personal Information**.
2. To download a CSV file of your login history for the past six months or your past 20,000 attempts, click **Download**.

Note: For security purposes, Salesforce can require users to pass a CAPTCHA user verification test to export data from their org. This simple text-entry test prevents malicious programs from accessing your org's data. To pass the test, users must correctly type the two words displayed in the overlay's text box. The words entered in the text box must be separated by a space.

Single Sign-On with SAML

If your organization uses SAML single sign-on identity provider certificates, single sign-on logins appear in the history.

My Domain

If you are using My Domain, you can identify which users are logging in with the new login URL and when. From Setup, enter *`Login History`* in the `Quick Find` box, then select **Login History** and view the Username and Login URL columns.

License Manager Users

The login history page sometimes includes internal users with names in the format *`033*********2@00d2********db`*. These users are associated with the License Management App (LMA), which manages the number of licenses used by a subscriber org. These internal users can appear in the License Management org (LMO) and in subscriber orgs in which an AppExchange package managed by the LMA is installed.

SEE ALSO:

Personalize Your Salesforce Experience

Identity Verification History

Identity Verification History

EDITIONS

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

As an admin, use Identity Verification History to monitor and audit up to 20,000 records of your org users' identity verification attempts from the past six months. For example, suppose that two-factor authentication is enabled when a user logs in. When the user successfully provides a time-based, one-time password as proof of identity, that information is recorded in Identity Verification History.

To access Identity Verification History, from Setup, enter *`Verification History`* in the `Quick Find` box, then select **Identity Verification History**. To view more information, such as the user's approximate geographic location at the time of verification, create a custom view and add the columns you want.

Identity Verification Fields

The following fields are displayed by default.

Field	Description
Time	The time of the identity verification attempt. The time zone is based on GMT.
Verification Attempt	ID of the verification attempt. Verification can involve several attempts and use different verification methods. For example, in a user's session, a user enters an invalid verification code (first attempt). The user then enters the correct code and successfully verifies identity (second attempt). Both attempts are part of a single verification and, therefore, have the same ID.
Username	The username of the user challenged for identity verification.
Activity Message	The text the user sees on the screen or in Salesforce Authenticator when prompted to verify identity. For example, if identity verification is required for a user's login, the user sees "You're trying to Log In to Salesforce". In this instance, the Activity Message is "Log In to Salesforce". The exception is when the User Activity is "Apex-defined activity." In this instance, the Activity Message can be a custom description passed by the Apex method. If the user is verifying identity using version 2 or later of the Salesforce Authenticator app, the custom description displays in the app as well as in Verification History. If the custom description isn't specified, the name of the Apex method is shown in Verification History. Note: If the user attempted to access a connected app, and the app was renamed or deleted after the verification attempt, this field shows the original connected app name.
Triggered By	The identity verification security policy or setting. • Apex method—Identity verification made by a verification Apex method.

Field	Description
	• Device activation—Identity verification required for users logging in from an unrecognized device or new IP address. This verification is part of Salesforce's risk-based authentication. • Lightning Login enrollment—Identity verification required for users enrolling in Lightning Login. This verification is triggered when the user attempts to enroll. Users are eligible to enroll if they have the "Lightning Login User" user permission and the org has enabled "Allow Lightning Login" in Session Settings. • High assurance session required—High assurance session required for resource access. This verification is triggered when the user tries to access a resource, such as a connected app, report, or dashboard that requires a high-assurance session level. • Lightning Login login—Identity verification required for users logging in via Lightning Login. This verification is triggered when the enrolled user attempts to log in. Users are eligible to log in if they have the "Lightning Login User" user permission, have successfully enrolled in Lightning Login, and the org has enabled "Allow Lightning Login" in Session Settings. • Profile session level policy—Session security level required at login. This verification is triggered by the "Session security level required at login" setting on the user's profile. • Two-factor authentication required—Two-factor authentication required at login. This verification is triggered by the "Two-Factor Authentication for User Interface Logins" user permission assigned to a custom profile. Or, the user permission is included in a permission set that is assigned to a user.
Method	The method by which the user attempted to verify identity in the verification event. • Email message—Salesforce sent an email with a verification code to the address associated with the user's account. • Lightning Login enrollment—Salesforce Authenticator sent a notification to the user's mobile device to enroll in Lightning Login. • One-time password—An authenticator app generated a time-based, one-time password (TOTP) on the user's mobile device. • Lightning Login login—Salesforce Authenticator sent a notification to the user's mobile device to approve login via Lightning Login. • Salesforce Authenticator—Salesforce Authenticator sent a notification to the user's mobile device to verify account activity.

Field	Description
	- Temporary verification code—A Salesforce admin or a user with the "Manage Two-Factor Authentication in User Interface" permission generated a temporary verification code for the user. - Text message—Salesforce sent a text message with a verification code to the user's mobile device. - U2F security key—A U2F security key generated required credentials for the user.
Status	The status of the identity verification attempt. - Access denied—The user denied the approval request in the authenticator app, such as Salesforce Authenticator. - Access denied: Flagged by user—The user denied the approval request in the authenticator app, such as Salesforce Authenticator, and also flagged the approval request to report to an administrator. - Failed: General error—An error caused by something other than an invalid verification code, too many verification attempts, or authenticator app connectivity. - Failed: Invalid verification code—The user provided an invalid verification code. - Failed: Recoverable error—Salesforce can't reach the authenticator app to verify identity, but will retry. - Failed: Too many attempts—The user attempted to verify identity too many times. For example, the user entered an invalid verification code repeatedly. - Succeeded—The user's identity was verified. - Succeeded: Automated response—Salesforce Authenticator approved the request for access because the request came from a trusted location. After users enable location services in Salesforce Authenticator, they can designate trusted locations. When a user trusts a location for a particular activity, such as logging in from a recognized device, that activity is approved from the trusted location for as long as the location is trusted. - User challenged; waiting for response—Salesforce challenged the user to verify identity and is waiting for the user to respond or for Salesforce Authenticator to send an automated response.
Login Time	Time of the login attempt, in GMT time zone.
Source IP	The IP address of the machine from which the user attempted the action that requires identity verification. For example, the IP address of the machine from where the user tried to log in or access reports. If it's a non-login action that required verification, the IP address

Field	Description
	can be different from the address from where the user logged in. This address can be an IPv4 or IPv6 address.
Location	The country where the user's IP address is physically located. This value is not localized. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.

You can display the following fields by creating a custom view. In the description, the IP address is the address of the machine from which the user attempted the action that requires identity verification. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.

Field	Description
City	The city where the user's IP address is physically located. This value is not localized.
Connected App	The name and link to the connected app the user attempted to access. If the connected app was renamed since the user's verification attempt, it shows the new name. If the connected app was deleted since the user's verification attempt, it shows "Unavailable."
Country	The country where the user's IP address is physically located. This value is not localized.
CountryIso	The ISO 3166 code for the country where the user's IP address is physically located. For more information, see Country Codes - ISO 3166
Latitude	The latitude where the user's IP address is physically located.
Login Type	The type of login, for example, Application, OAuth, or SAML.
Longitude	The longitude where the user's IP address is physically located.
Postal Code	The postal code where the user's IP address is physically located. This value is not localized.
Subdivision	The name of the subdivision where the user's IP address is physically located. In the U.S., this value is usually the state name (for example, Pennsylvania). This value is not localized.
User Activity	The action the user attempted that requires identity verification. • Access a connected app—The user attempted to access a connected app. • Access reports—The user attempted to access reports or dashboards. • Apex-defined activity—The user attempted to access a Salesforce resource with a verification Apex method.

Field	Description
	- Export and print reports—The user attempted to export or print reports or dashboards. - Log in to Salesforce—The user attempted to log in.

SEE ALSO:

Monitor Login History

Delegate Two-Factor Authentication Management Tasks

Monitor Login Activity with Login Forensics

EDITIONS

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

Login forensics helps administrators better determine which user behavior is legitimate to prevent identity fraud in Salesforce.

Companies continue to view identity fraud as a major concern. Given the number of logins to an org on a daily—even hourly—basis, security practitioners can find it challenging to determine if a specific user account is compromised.

Login forensics helps you identify suspicious login activity. It provides you key user access data, including:

- The average number of logins per user per a specified time period
- Who logged in more than the average number of times
- Who logged in during non-business hours
- Who logged in using suspicious IP ranges

There's some basic terminology to master before using this feature.

Event

An event refers to anything that happens in Salesforce, including user clicks, record state changes, and taking measurements of various values. Events are immutable and timestamped.

Login Event

A single instance of a user logging in to an organization. Login events are similar to login history in Salesforce. However, you can add `HTTP` header information to login events, which makes them extensible.

Login History

The login history that administrators can obtain by downloading the information to `.cvs` or `.gzip` file and that's available through Setup and the API. This data has indexing and history limitations.

Administrators can track events using the LoginEvent object. There's no user interface for login forensics. Use the Force.com IDE, Workbench, or other development tools to interact with this feature.

IN THIS SECTION:

Considerations for Using Login Forensics

Before you get started with login forensics, keep in mind some considerations for use.

Enable Login Forensics

Perform this quick, one time setup to start collecting data about your org's login events.

Considerations for Using Login Forensics

EDITIONS

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

Before you get started with login forensics, keep in mind some considerations for use.

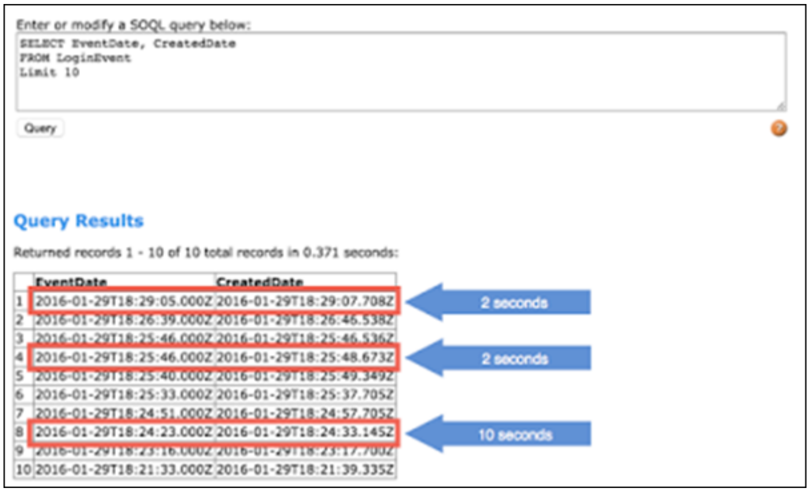
- This feature is API only. You can't view events in the user interface.
- Login events are retained for 10 years by default.
- Because login forensics uses an asynchronous queuing technology similar to `@future` calls in Apex, login data can be delayed when querying.

How Does Login Forensics Compare to Login History and Login Log Lines?

Feature	Login Forensics	Login History	Login Log Lines
Standard Object or File	LoginEvent	LoginHistory	EventLogFile (Login event type)
Data Duration Until Deleted	10 years	6 months	30 days
Storage	HBase	Oracle	Oracle
Access	API	Setup UI, API	API download, Wave dashboard
Permissions	View Login Forensics Events	Manage Users	View Event Log Files
Extensibility	Yes, using AdditionalInfo field	No	No
Packaging	Included with Event Monitoring add-on	Included with all orgs	Included with Event Monitoring add-on

Are Events Captured in Near Real Time?

Yes. But what does "near real time" mean? It means that there can be a minor delay from when the event occurred and when you can query it. You can monitor the near-real-time nature of your events. Take the average difference between the EventDate and the CreatedDate fields to see when your events were captured. This example in Workbench shows the time differences.



Enter or modify a SOQL query below:

```
SELECT EventDate, CreatedDate
FROM LoginEvent
Limit 10
```

Query Results

Returned records 1 - 10 of 10 total records in 0.371 seconds:

	EventDate	CreatedDate
1	2016-01-29T18:29:05.000Z	2016-01-29T18:29:07.708Z
2	2016-01-29T18:26:39.000Z	2016-01-29T18:26:46.538Z
3	2016-01-29T18:25:46.000Z	2016-01-29T18:25:46.536Z
4	2016-01-29T18:25:46.000Z	2016-01-29T18:25:48.673Z
5	2016-01-29T18:25:40.000Z	2016-01-29T18:25:49.349Z
6	2016-01-29T18:25:33.000Z	2016-01-29T18:25:37.705Z
7	2016-01-29T18:24:51.000Z	2016-01-29T18:24:57.705Z
8	2016-01-29T18:24:23.000Z	2016-01-29T18:24:33.145Z
9	2016-01-29T18:23:16.000Z	2016-01-29T18:23:17.700Z
10	2016-01-29T18:21:33.000Z	2016-01-29T18:21:39.335Z

Enable Login Forensics

Perform this quick, one time setup to start collecting data about your org’s login events.

You can enable login forensics from the Event Monitoring Setup page in the Setup area.

USER PERMISSIONS

To enable login forensics

- Modify All Data

Monitor Training History

As an administrator, you want to know that your team is learning how to use Salesforce effectively. The Training Class History shows you all of the Salesforce training classes your users have taken.

Administrators can view the Training Class History from Setup by entering *`Training History`* in the `Quick Find` box, then selecting **Training History**. After taking a live training class, users must submit the online training feedback form to have their training attendance recorded in the training history.

> Note: If you don’t see this link under **Manage Users**, your organization has been migrated to a new system. You need to be a Help & Training Admin to access the training reports via My Cases in Help & Training. Contact Salesforce if you do not have this access.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view training history:

- Manage Users

Monitor Setup Changes

Setup Audit Trail tracks the recent setup changes that you and other admins have made to your org. Audit history is especially useful in orgs with multiple admins.

To view the audit history, from Setup, enter *`View Setup Audit Trail`* in the `Quick Find` box, then select **View Setup Audit Trail**. To download your org’s full setup history for the past 180 days, click **Download**.

The history shows the 20 most recent setup changes made to your org. It lists the date of the change, who made it, and what the change was. If a delegate (like an admin or customer support representative) makes a setup change on behalf of an end user, the Delegate User column shows the delegate’s username. For example, if a user grants login access to an admin and the admin makes a setup change, the admin’s username is listed.

Setup Audit Trail tracks these changes.

Setup	Changes Tracked
Administration	• Company information, default settings like language or locale, and company messages • Multiple currency • Users, portal users, roles, permission sets, and profiles • Email addresses for any user

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view audit trail history:

- View Setup and Configuration

Setup	Changes Tracked
	• Deleting email attachments sent as links • Email footers, including creating, editing, or deleting • Record types, including creating or renaming record types and assigning record types to profiles • Divisions, including creating, editing, and transferring and changing users' default division • Certificates, adding or deleting • Domain names • Enabling or disabling Salesforce as an identity provider
Customization	• User interface settings like collapsible sections, Quick Create, hover details, or related list hover links • Page layout, action layout, and search layouts • Compact layouts • Salesforce app navigation menu • Inline edits • Custom fields and field-level security, including formulas, picklist values, and field attributes like the auto-number field format, field manageability, or masking of encrypted fields • Lead settings, lead assignment rules, and lead queues • Activity settings • Support settings, business hours, case assignment and escalation rules, and case queues • Requests to Salesforce Customer Support • Tab names, including tabs that you reset to the original tab name • Custom apps (including Salesforce console apps), custom objects, and custom tabs • Contract settings • Forecast settings • Email-to-Case or On-Demand Email-to-Case, enabling or disabling • Custom buttons, links, and s-controls, including standard button overrides • Drag-and-drop scheduling, enabling or disabling • Similar opportunities, enabling, disabling, or customizing • Quotes, enabling or disabling • Data category groups, data categories, and category-group assignments to objects • Article types • Category groups and categories • Salesforce Knowledge settings • Ideas settings • Answers settings • Field tracking in feeds • Campaign influence settings • Critical updates, activating or deactivating • Chatter email notifications, enabling or disabling • Chatter new user creation settings for invitations and email domains, enabling or disabling

Setup	Changes Tracked
	• Validation rules
Security and Sharing	• Public groups, sharing rules, and org-wide sharing, including the Grant Access Using Hierarchies option • Password policies • Password resets • Session settings, like session timeout (excluding **Session times out after** and **Session security level required at login** profile settings) • Delegated administration groups and the items delegated admins can manage (setup changes made by delegated administrators are also tracked) • Lightning Login, enabling or disabling, enrollments, and cancellations • How many records a user emptied from their Recycle Bin and from the org's Recycle Bin • SAML (Security Assertion Markup Language) configuration settings • Salesforce certificates • Identity providers, enabling or disabling • Named credentials • Service providers • Shield Platform Encryption setup
Data Management	• Mass delete use, including when a mass delete exceeds the user's Recycle Bin limit on deleted records • Data export requests • Mass transfer use • Reporting snapshots, including defining, deleting, or changing the source report or target object on a reporting snapshot • Use of the Data Import Wizard • Sandbox deletions
Development	• Apex classes and triggers • Visualforce pages, custom components, and static resources • Lightning pages • Action link templates • Custom settings • Custom metadata types and records • Remote access definitions • Force.com Sites settings
Various Setup	• API usage metering notification, creating • Territories • Process automation settings • Approval processes • Workflow actions, creating or deleting

Setup	Changes Tracked
	• Visual Workflow files • Packages from Force.com AppExchange that you installed or uninstalled
Using the application	• Account team and opportunity team selling settings • Activating Google Apps services • Mobile configuration settings, including data sets, mobile views, and excluded fields • Users with the "Manage External Users" permission logging in to the partner portal as partner users • Users with the "Edit Self-Service Users" permission logging in to the Salesforce Customer Portal as Customer Portal users • Partner portal accounts, enabling or disabling • Salesforce Customer Portal accounts, disabling • Salesforce Customer Portal, enabling or disabling • Creating multiple Customer Portals • Entitlement processes and entitlement templates, changing or creating • Self-registration for a Salesforce Customer Portal, enabling or disabling • Customer Portal or partner portal users, enabling or disabling

SEE ALSO:

Security Health Check

Field History Tracking

You can select certain fields to track and display the field history in the History related list of an object. The field history data is retained for up to 18 months.

You can track the field history of custom objects and the following standard objects.

- Accounts
- Articles
- Assets
- Campaigns
- Cases
- Contacts
- Contracts
- Contract line items
- Entitlements
- Leads
- Opportunities
- Orders
- Order Products
- Products

EDITIONS

Available in: Salesforce Classic, Lightning Experience, and the Salesforce app

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

Standard Objects are not available in **Database.com**

- Service Contracts
- Solutions

Modifying any of these fields adds an entry to the History related list. All entries include the date, time, nature of the change, and who made the change. Not all field types are available for historical trend reporting. Certain changes, such as case escalations, are always tracked.

Note: Field history increases beyond your current limits require purchasing the Field Audit Trail add-on following the Spring '15 release. When the add-on subscription is enabled, your field history storage is changed to reflect the retention policy associated with the offering. If your org was created before June 2011 and your field history limits remain static, Salesforce commits to retain your field history without a limit. If your org was created after June 2011 and you decide not to purchase the add-on, field history is guaranteed to be retained for 18 months.

Consider the following when working with field history tracking.

- Changes to fields with more than 255 characters are tracked as edited, and their old and new values are not recorded.
- Tracked field values are not automatically translated; they display in the language in which they were made. For example, if a field is changed from *Green* to *Verde*, *Verde* is displayed no matter what a user's language is, unless the field value has been translated into other languages via the Translation Workbench. This also applies to record types and picklist values.
- Changes to custom field labels that have been translated via the Translation Workbench are shown in the locale of the user viewing the History related list. For example, if a custom field label is Red and translated into Spanish as Rojo, then a user with a Spanish locale sees the custom field label as Rojo. Otherwise, the user sees the custom field label as Red.
- Changes to date fields, number fields, and standard fields are shown in the locale of the user viewing the History related list. For example, a date change to *August 5, 2012* shows as *8/5/2012* for a user with the English (United States) locale, and as *5/8/2012* for a user with the English (United Kingdom) locale.
- If a trigger causes a change on an object the current user doesn't have permission to edit, that change is not tracked because field history honors the permissions of the current user.

IN THIS SECTION:

Track Field History for Standard Objects

You can enable field history tracking for standard objects in the object's management settings.

Track Field History for Custom Objects

You can enable field history tracking for custom objects in the object's management settings.

Disable Field History Tracking

You can turn off field history tracking from the object's management settings.

Field Audit Trail

Field Audit Trail lets you define a policy to retain archived field history data up to 10 years, independent of field history tracking. This feature helps you comply with industry regulations related to audit capability and data retention.

SEE ALSO:

Track Field History for Standard Objects

Track Field History for Custom Objects

Field Audit Trail

Disable Field History Tracking

Track Field History for Standard Objects

You can enable field history tracking for standard objects in the object's management settings.

If you use both business accounts and person accounts, review the following before enabling account field history tracking:

- Field history tracking for accounts affects both business accounts and person accounts.
- Enabling field history tracking on person accounts does not enable field history tracking on personal contacts.

To set up field history tracking:

1. From the management settings for the object whose field history you want to track, go to the fields area.
2. Click **Set History Tracking**.

   Tip: When you enable tracking for an object, customize your page layouts to include the object's history related list.

3. For accounts, contacts, leads, and opportunities, select the `Enable Account History`, `Enable Contact History`, `Enable Lead History`, or `Enable Opportunity History` checkbox.
4. Choose the fields you want tracked.

   You can select a combination of up to 20 standard and custom fields per object. This limit includes fields on business accounts and person accounts.

   Certain changes, such as case escalations, are always tracked.

   You can't track the following fields:

   - Formula, roll-up summary, or auto-number fields
   - `Created By` and `Last Modified By`
   - `Expected Revenue` field on opportunities
   - `Master Solution Title` or the `Master Solution Details` fields on solutions; these fields display only for translated solutions in organizations with multilingual solutions enabled.

5. Click **Save**.

   Salesforce tracks history from this date and time forward. Changes made prior to this date and time are not included.

EDITIONS

Available in: Salesforce Classic, Lightning Experience, and the Salesforce app

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

Standard Objects are not available in **Database.com**

USER PERMISSIONS

To set up which fields are tracked:

- Customize Application

SEE ALSO:

Field History Tracking

Track Field History for Custom Objects

You can enable field history tracking for custom objects in the object's management settings.

1. From the management settings for the custom object, click **Edit**.
2. Select the `Track Field History` checkbox.

   Tip: When you enable tracking for an object, customize your page layouts to include the object's history related list.

3. Save your changes.
4. Click `Set History Tracking` in the Custom Fields & Relationships section.

   This section lets you set a custom object's history for both standard and custom fields.

5. Choose the fields you want tracked.

   You can select up to 20 standard and custom fields per object. You can't track:

   - Formula, roll-up summary, or auto-number fields
   - `Created By` and `Last Modified By`

6. Click **Save**.

   Salesforce tracks history from this date and time forward. Changes made prior to this date and time are not included.

SEE ALSO:

Field History Tracking

Find Object Management Settings

EDITIONS

Available in: Salesforce Classic, Lightning Experience, and the Salesforce app

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

Standard Objects are not available in **Database.com**

USER PERMISSIONS

To set up which fields are tracked:

- Customize Application

Disable Field History Tracking

You can turn off field history tracking from the object's management settings.

Note: You can't disable field history tracking for an object if Apex references one of its a field on the object is referenced in Apex.

1. From the management settings for the object whose field history you want to stop tracking, go to Fields.
2. Click `Set History Tracking`.
3. Deselect **Enable History** for the object you are working with—for example, **Enable Account History**, **Enable Contact History**, **Enable Lead History**, or **Enable Opportunity History**.

   The History related list is automatically removed from the associated object's page layouts.

   If you disable field history tracking on a standard object, you can still report on its history data up to the date and time that you disabled tracking. If you disable field history tracking on a custom object, you cannot report on its field history.
4. Save your changes.

SEE ALSO:

Field History Tracking

Find Object Management Settings

EDITIONS

Available in: Salesforce Classic, Lightning Experience, and the Salesforce app

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

Standard Objects are not available in **Database.com**

USER PERMISSIONS

To set up which fields are tracked:

- Customize Application

Field Audit Trail

Field Audit Trail lets you define a policy to retain archived field history data up to 10 years, independent of field history tracking. This feature helps you comply with industry regulations related to audit capability and data retention.

Use Salesforce Metadata API to define a retention policy for your field history. Then use REST API, SOAP API, and Tooling API to work with your archived data. For information about enabling Field Audit Trail, contact your Salesforce representative.

Field history is copied from the History related list into the `FieldHistoryArchive` object and then deleted from the History related list. You define one `HistoryRetentionPolicy` for your related history lists, such as Account History, to specify Field Audit Trail retention policies for the objects you want to archive. You can then deploy the object by using the Metadata API (Workbench or Force Migration Tool). You can update the retention policy on an object as often as you like.

You can set field history retention policies on the following objects.

- Accounts
- Cases
- Contacts
- Leads
- Opportunities
- Assets
- Entitlements

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To specify a field history retention policy:

- Retain Field History

- Service Contracts
- Contract Line Items
- Solutions
- Products
- Price Books
- Custom objects with field history tracking enabled

Note: `HistoryRetentionPolicy` is automatically set on the above objects, once Field Audit Trail is enabled. By default, data is archived after 18 months in a production organization, after one month in a sandbox organization, and all archived data is stored for 10 years. The default retention policy is not included when retrieving the object's definition through the Metadata API. Only custom retention policies are retrieved along with the object definition.

You can include field history retention policies in managed and unmanaged packages.

The following fields can't be tracked.

- Formula, roll-up summary, or auto-number fields
- Created By and Last Modified By
- Expected Revenue field on opportunities
- Master Solution Title or the Master Solution Details fields on solutions
- Long text fields
- Multi-select fields

After you define and deploy a Field Audit Trail policy, production data is migrated from related history lists such as Account History into the `FieldHistoryArchive` object. The first copy writes the field history that's defined by your policy to archive storage and sometimes takes a long time. Subsequent copies transfer only the changes since the last copy and are much faster. A bounded set of SOQL is available to query your archived data.

Note: If your organization has Field Audit Trail enabled, previously archived data isn't encrypted if you turn on Platform Encryption later. For example, your organization uses Field Audit Trail to define a data history retention policy for an account field, such as the phone number field. After enabling Platform Encryption, you turn on encryption for that field, and phone number data in the account is encrypted. New phone number records and previous updates stored in the Account History related list are encrypted. However, phone number history data that is already archived in the `FieldHistoryArchive` object continues to be stored without encryption. If your organization needs to encrypt previously archived data, contact Salesforce. We will encrypt and rearchive the stored field history data, then delete the unencrypted archive.

IN THIS SECTION:

Examples

SEE ALSO:

SOAP API Developer Guide: FieldHistoryArchive

Metadata API Developer Guide: HistoryRetentionPolicy

ISVforce Guide: Overview of Packages

Force.com SOQL and SOSL Reference: SOQL with Archived Data

Examples

Set Data Retention Policy for Field History

This example demonstrates how to set a field history data retention policy by using Metadata API. You need to edit the metadata only if you want to override the default policy values (18 months of production storage and 10 years of archive storage). Setting data retention policy involves creating a metadata package and deploying it. The package consists of a `.zip` file that contains an `objects` folder with the XML that defines each object's retention policy, and a project manifest that lists the objects and the API version to use.

Note: The first copy writes the entire field history that's defined by your policy to archive storage and might take a long time. Subsequent copies transfer only the changes since the last copy, and will be much faster.

1. Define a field history data retention policy for each object. The policy specifies the number of months that you want to maintain field history in Salesforce, and the number of years that you want to retain field history in the archive. The following sample file defines a policy of archiving the object after six months, and keeping the archives for five years.

```
<?xml version="1.0" encoding="UTF-8"?>
<CustomObject xmlns="http://soap.sforce.com/2006/04/metadata">
   <historyRetentionPolicy>
       <archiveAfterMonths>6</archiveAfterMonths>
       <archiveRetentionYears>5</archiveRetentionYears>
       <description>My field history retention</description>
   </historyRetentionPolicy>
   <fields>
       <fullName>AccountSource</fullName>
...
</CustomObject>
```

   The file name determines the object to which the policy is applied. For example, to apply the above policy to the Account object, save the file as `Account.object`. For existing custom objects, this works the same way, with the file named after the custom object. For example: `myObject__c.object`.

2. Create the project manifest, which is an XML file that's called `package.xml`. The following sample file lists several objects for which data retention policy is to be applied. With this manifest file, you expect the objects folder to contain five files: `Account.object`, `Case.object`, and so on.

```
<?xml version="1.0" encoding="UTF-8"?>
<Package xmlns="http://soap.sforce.com/2006/04/metadata">
    <types>
        <members>Account</members>
        <members>Case</members>
        <members>Contact</members>
        <members>Lead</members>
        <members>Opportunity</members>
    </types>
    <version>32.0</version>
</Package>
```

3. Create the `.zip` file and use the `deploy()` function to deploy your changes to your production environment. For more information, see the Metadata API Guide.

   Note: This pilot doesn't support deployment from sandbox to production environments.

That's it! Your field history retention policy will go into effect according to the time periods that you set.

Create a Custom Object and Set Field History Retention Policy at the Same Time

You can use Metadata API to create a custom object and set retention policy at the same time. You must specify the minimum required fields when creating a new custom object. Here's sample XML that creates an object and sets field history retention policy:

```
<?xml version="1.0" encoding="UTF-8"?>
<CustomObject xmlns="http://soap.sforce.com/2006/04/metadata">
    <deploymentStatus>Deployed</deploymentStatus>
    <enableHistory>true</enableHistory>
    <description>just a test object with one field for eclipse ide testing</description>
    <historyRetentionPolicy>
        <archiveAfterMonths>3</archiveAfterMonths>
        <archiveRetentionYears>10</archiveRetentionYears>
        <gracePeriodDays>1</gracePeriodDays>
        <description>Transaction Line History</description>
    </historyRetentionPolicy>
    <fields>
        <fullName>Comments__c</fullName>
        <description>add your comments about this object here</description>
       <inlineHelpText>This field contains comments made about this object</inlineHelpText>

        <label>Comments</label>
        <length>32000</length>
        <trackHistory>true</trackHistory>
        <type>LongTextArea</type>
        <visibleLines>30</visibleLines>
    </fields>
    <label>MyFirstObject</label>
    <nameField>
        <label>MyFirstObject Name</label>
        <type>Text</type>
    </nameField>
    <pluralLabel>MyFirstObjects</pluralLabel>
    <sharingModel>ReadWrite</sharingModel>
</CustomObject>
```

Set `trackHistory` to `true` on the fields that you want to track and `false` on the other fields.

Update Data Retention Policy for Field History

If a field history data retention policy is already defined on an object, you can update the policy by specifying a new value of `HistoryRetentionPolicy` in the metadata for that object. Once you deploy the metadata changes, the new policy overwrites the old one.

Note: To check the current data retention policy for any object, retrieve its metadata using Metadata API and look up the value of `HistoryRetentionPolicy`.

Query Archived Data

You can retrieve archived data by making SOQL queries on the `FieldHistoryArchive` object. You can filter on the `FieldHistoryType`, `ParentId`, and `CreatedDate` fields, as long as you specify them in that order. For example:

```
SELECT ParentId, FieldHistoryType, Field, Id, NewValue, OldValue FROM FieldHistoryArchive
 WHERE FieldHistoryType = ‘Account’ AND ParentId=’906F000000
```

SEE ALSO:

Metadata API Developer Guide: deploy()

Metadata API Developer Guide: CustomObject

Force.com SOQL and SOSL Reference: SOQL with Archived Data

Monitor Debug Logs

Set trace flags to trigger logging for users, Apex classes, and Apex triggers in the Developer Console or in Setup. Monitor the resulting logs to diagnose problems in your org.

You can retain and manage debug logs for specific users, including yourself, and for classes and triggers. Setting class and trigger trace flags doesn't cause logs to be generated or saved. Class and trigger trace flags override other logging levels, including logging levels set by user trace flags, but they don't cause logging to occur. If logging is enabled when classes or triggers execute, logs are generated at the time of execution.

IN THIS SECTION:

Set Up Debug Logging

To activate debug logging for users, Apex classes, and Apex triggers, configure trace flags and debug levels in the Developer Console or in Setup. Each trace flag includes a debug level, start time, end time, and log type. The trace flag's log type specifies the entity you're tracing.

View Debug Logs

The debug log contains information about each transaction, such as whether it was successful and how long it took. Depending on the filters set by your trace flags, the log can contain varying levels of detail about the transaction.

EDITIONS

Available in: Salesforce Classic

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

The Salesforce user interface and Email Services are not available in **Database.com**.

USER PERMISSIONS

To view, retain, and delete debug logs:

- Manage Users

  OR

  View All Data

Set Up Debug Logging

To activate debug logging for users, Apex classes, and Apex triggers, configure trace flags and debug levels in the Developer Console or in Setup. Each trace flag includes a debug level, start time, end time, and log type. The trace flag's log type specifies the entity you're tracing.

You can retain and manage debug logs for specific users, including yourself, and for classes and triggers. Setting class and trigger trace flags doesn't cause logs to be generated or saved. Class and trigger trace flags override other logging levels, including logging levels set by user trace flags, but they don't cause logging to occur. If logging is enabled when classes or triggers execute, logs are generated at the time of execution.

The following are the limits for debug logs.

- Each debug log must be 2 MB or smaller. Debug logs that are larger than 2 MB are reduced in size by removing older log lines, such as log lines for earlier `System.debug` statements. The log lines can be removed from any location, not just the start of the debug log.
- Debug logs are retained for 7 days.
- If you generate more than 250 MB of debug logs in a 15-minute window, your trace flags are disabled. We send an email to the users who last modified the trace flags, informing them that they can re-enable the trace flag in 15 minutes.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view, retain, and delete debug logs:

- Manage Users

  OR

  View All Data

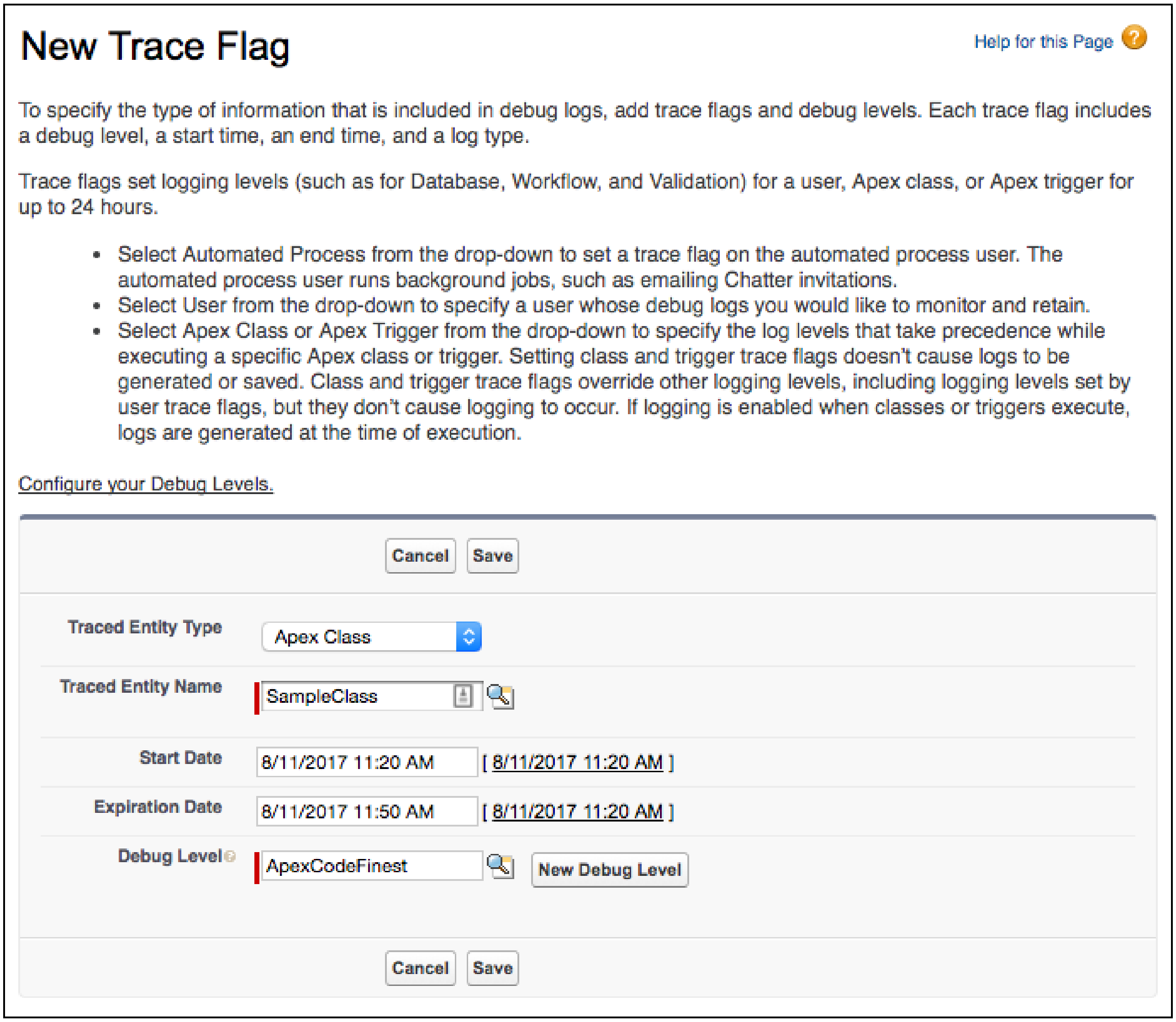
Configure Trace Flags in the Developer Console

To configure trace flags and debug levels from the Developer Console, click **Debug** > **Change Log Levels**. Then complete these actions.

- To create a trace flag, click **Add**.
- To edit an existing trace flag's duration, double-click its start or end time.
- To change a trace flag's debug level, click **Add/Change** in the Debug Level Action column. You can then edit your existing debug levels, create or delete a debug level, and assign a debug level to your trace flag. Deleting a debug level deletes all trace flags that use it.

Create Trace Flags in Setup

1. From Setup, enter *`Debug Logs`* in the `Quick Find` box, then click **Debug Logs**.
2. Click **New**.
3. Select the entity to trace, the time period during which you want to collect logs, and a debug level. A debug level is a set of log levels for debug log categories: Database, Workflow, Validation, and so on. You can reuse debug levels across your trace flags.



New Trace Flag

To specify the type of information that is included in debug logs, add trace flags and debug levels. Each trace flag includes a debug level, a start time, an end time, and a log type.

Trace flags set logging levels (such as for Database, Workflow, and Validation) for a user, Apex class, or Apex trigger for up to 24 hours.

- Select Automated Process from the drop-down to set a trace flag on the automated process user. The automated process user runs background jobs, such as emailing Chatter invitations.
- Select User from the drop-down to specify a user whose debug logs you would like to monitor and retain.
- Select Apex Class or Apex Trigger from the drop-down to specify the log levels that take precedence while executing a specific Apex class or trigger. Setting class and trigger trace flags doesn't cause logs to be generated or saved. Class and trigger trace flags override other logging levels, including logging levels set by user trace flags, but they don't cause logging to occur. If logging is enabled when classes or triggers execute, logs are generated at the time of execution.

Configure your Debug Levels.

Traced Entity Type	Apex Class
Traced Entity Name	SampleClass
Start Date	8/11/2017 11:20 AM [8/11/2017 11:20 AM]
Expiration Date	8/11/2017 11:50 AM [8/11/2017 11:20 AM]
Debug Level	ApexCodeFinest

View, Edit, or Delete Trace Flags in Setup

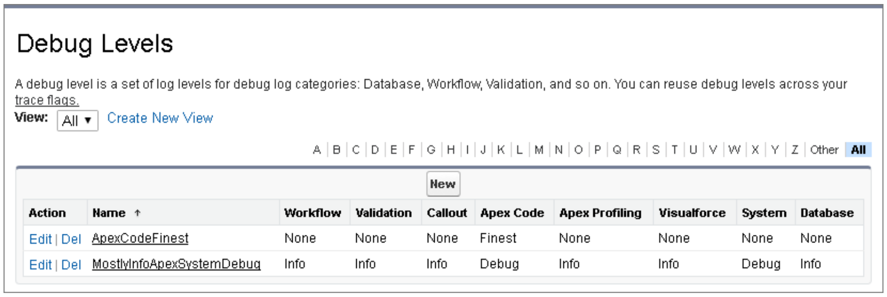
To manage trace flags from Setup, complete these actions.

1. Navigate to the appropriate Setup page.
   - For user-based trace flags, enter *Debug Logs* in the `Quick Find` box, then click **Debug Logs**.
   - For class-based trace flags, enter *Apex Classes* in the `Quick Find` box, click **Apex Classes**, click the name of a class, then click **Trace Flags**.
   - For trigger-based trace flags, enter *Apex Triggers* in the `Quick Find` box, click **Apex Triggers**, click the name of a trigger, then click **Trace Flags**.
2. From the Setup page, click an option in the Action column.
   - To delete a trace flag, click **Delete**.
   - To modify a trace flag, click **Edit**.
   - To modify a trace flag's debug level, click **Filters**.

- To create a debug level, click **Edit**, and then click **New Debug Level**.

Configure Debug Levels in Setup

To manage your debug levels from Setup, enter *Debug Levels* in the Quick Find box, then click **Debug Levels**. To edit or delete a debug level, click an option in the Action column. To create a debug level, click **New**.


View: All ▾
Create New View
A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | Other | All
New

Debug Levels

A debug level is a set of log levels for debug log categories: Database, Workflow, Validation, and so on. You can reuse debug levels across your trace flags.

Action	Name ↑	Workflow	Validation	Callout	Apex Code	Apex Profiling	Visualforce	System	Database
Edit | Del	ApexCodeFinest	None	None	None	Finest	None	None	None	None
Edit | Del	MostlyInfoApexSystemDebug	Info	Info	Info	Debug	Info	Info	Debug	Info

Collect Debug Logs for Guest Users

Your public users generate a large volume of events, which can quickly fill up your debug logs. For this reason, logs are collected for site visitors who are using your Guest User license only when a public user's browser has a special cookie. Logging of public users' asynchronous activity isn't available because asynchronous requests don't include browser cookies.

To enable logging for a guest user's synchronous activity:

1. Ask the user to set a browser cookie with a domain of `.force.com`, a name of `debug_logs`, and any value. (If you use a custom domain, ask your user to set the cookie for your domain rather than for `.force.com`.) Refer to the documentation for your user's browser for information on adding cookies. To add cookies, your user probably needs a browser plug-in or extension for web development.

   - To set a cookie for API requests made with Java code, use the `URLConnection` class and set the cookie value as follows.

     - If you use a `.force.com` domain, use this code.

       ```
       URL url = new URL("http://yourSite.force.com/");
       URLConnection con = url.openConnection();
       con.setDoOutput(true);
       con.setRequestProperty("Cookie", "debug_logs=debug_logs,domain=.force.com");
       con.setRequestProperty("Content-Type", "text/plain; charset=utf-8");
       con.connect();
       ```

     - If you use a custom domain (for example, `yourCustomDomain.com`), use this code.

       ```
       URL url = new URL("http://yourCustomDomain.com/");
       URLConnection con = url.openConnection();
       con.setDoOutput(true);
       con.setRequestProperty("Cookie", "debug_logs=debug_logs,domain=.force.com");
       con.setRequestProperty("Content-Type", "text/plain; charset=utf-8");
       con.connect();
       ```

   - To set a browser cookie in Google Chrome™:

     a. Navigate to your site.

     b. Open the Chrome DevTools Console by pressing Ctrl+Shift+J (Cmd+Opt+J on macOS).

     c. Execute a command to set the cookie.

    - If you use a `.force.com` domain, use this command.

      ```
      document.cookie="debug_logs=debug_logs;domain=.force.com";
      ```

    - If you use a custom domain (for example, `yourCustomDomain.com`), use this command.

      ```
      document.cookie="debug_logs=debug_logs;domain=yourCustomDomain.com";
      ```

  - To set a browser cookie in other browsers, install a plug-in or extension.

2. Find the name of your site's guest user.
   a. From Setup, enter *`Sites`* in the `Quick Find` box, then select **Sites**.
   b. Select your site from the Site Label column.
   c. Select **Public Access Settings** > **View Users**.

3. Set a user-based trace flag on the guest user.
   a. From Setup, enter *`Debug Logs`* in the `Quick Find` box, then click **Debug Logs**.
   b. Click **New**.
   c. Set the traced entity type to **User**.
   d. Open the lookup for the Traced Entity Name field, and then find and select your guest user.
   e. Assign a debug level to your trace flag.
   f. Click **Save**.

Tip: Debug logs are for live troubleshooting. To record all site traffic, use event monitoring. For details, see the Sites section of *SOAP API Developer Guide*: EventLogFile.

SEE ALSO:

Monitor Debug Logs

View Debug Logs

USER PERMISSIONS

To use the Developer Console:	API Enabled AND View All Data
To execute anonymous Apex:	Author Apex
To use code search and run SOQL or SOSL on the query tab:	API Enabled
To save changes to Apex classes and triggers:	Author Apex
To save changes to Visualforce pages and components:	Customize Application
To save changes to Lightning resources:	Customize Application

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

The debug log contains information about each transaction, such as whether it was successful and how long it took. Depending on the filters set by your trace flags, the log can contain varying levels of detail about the transaction.

To view a debug log, from Setup, enter `Debug Logs` in the `Quick Find` box, then select **Debug Logs**. Then click **View** next to the debug log that you want to examine. Click **Download** to download the log as an XML file.

The following are the limits for debug logs.

- Each debug log must be 2 MB or smaller. Debug logs that are larger than 2 MB are reduced in size by removing older log lines, such as log lines for earlier `System.debug` statements. The log lines can be removed from any location, not just the start of the debug log.
- Debug logs are retained for 7 days.
- If you generate more than 250 MB of debug logs in a 15-minute window, your trace flags are disabled. We send an email to the users who last modified the trace flags, informing them that they can re-enable the trace flag in 15 minutes.

SEE ALSO:

Monitor Debug Logs

Monitoring Scheduled Jobs

The All Scheduled Jobs page lists all reporting snapshots, scheduled Apex jobs, and dashboards scheduled to refresh.

To view this page, from Setup, enter `Scheduled Jobs` in the `Quick Find` box, then select **Scheduled Jobs**. Depending on your permissions, you can perform some or all of the following actions.

- Click **Del** to permanently delete all instances of a scheduled job.
- View the details of a scheduled job, such as the:
  - Name of the scheduled job
  - Name of the user who submitted the scheduled job
  - Date and time at which the scheduled job was originally submitted
  - Date and time at which the scheduled job started
  - Next date and time at which the scheduled job will run
  - Type of scheduled job

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Reporting Snapshots and Dashboards are not available in **Database.com**

USER PERMISSIONS

To monitor scheduled jobs:

- View Setup and Configuration

Monitoring Background Jobs

You can monitor background jobs in your organization, such as when parallel sharing recalculation is running.

Parallel sharing recalculation helps larger organizations to speed up sharing recalculation of each object. If the number of impacted records from an owner-based sharing rule insert or update is less than 25,000, recalculation runs synchronously and you won't receive an email notification when it's completed. Owner-based sharing rule inserts and updates impacting less than 25,000 records are not available on the Background Jobs page.

To view any background jobs in your organization, from Setup, enter *`Background Jobs`* in the `Quick Find` box, then select **Background Jobs**.

The Background Jobs page shows the details of background jobs, including a percentage estimate of the recalculation progress. The **Job Type** column shows the background job that's running, such as `Organization-Wide Default Update`. The **Job Sub Type** column shows the affected object, such as `Account` or `Opportunity`.

Note: You can only monitor background jobs on this page. Contact Salesforce to abort a background job.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To monitor background jobs:

- View Setup and Configuration

SEE ALSO:

Recalculate Sharing Rules

Asynchronous Parallel Recalculation of Sharing Rules

Enable Your Users to Work on Mobile Devices

Salesforce provides several mobile apps to keep you and your users connected and productive, no matter where you are.

IN THIS SECTION:

Put the Salesforce App In Your Users' Hands

The Salesforce app enables your users to stay productive on the go.

Help Users From Anywhere With SalesforceA

SalesforceA is a mobile app for Salesforce administrators. When you're away from your desk, you can use your phone or tablet to perform essential administration tasks like resetting passwords, freezing users, and viewing current system status.

Salesforce Chatter

Salesforce Chatter is a downloadable app for Windows 10 Anniversary Edition users. Salesforce Chatter combines Chatter feeds and posting functionality with the power of an app optimized for Windows 10 users.

Support On-the-Go Productivity with Salesforce Mobile Classic

Salesforce Mobile Classic helps your teams succeed by allowing users to access their latest Salesforce data, whenever and wherever they need it, directly from Android™ and iPhone® devices.

View a Mobile User's Push Registration Information

With the Mobile Push Registrations Page, you can view any user's push registration information for general troubleshooting.

Put the Salesforce App In Your Users' Hands

The Salesforce app enables your users to stay productive on the go.

IN THIS SECTION:

Salesforce App Setup Options

See the many options for customizing the Salesforce app, to make it an effective on-the-go tool for your users' business needs.

Set Up the Salesforce App with the Salesforce Mobile Wizard

The Salesforce Mobile Wizard provides an easy way to complete the essential setup tasks. After you've set up Salesforce with this wizard, your sales reps can use Salesforce to run their business from their mobile devices.

Control Access to the Salesforce App

You can control your organization's access to Salesforce for Android and Salesforce for iOS and Salesforce mobile web.

Salesforce App and Password Manager Apps

Good security practices require long, complex passwords. But typing long, complex passwords on small mobile keyboards is error prone and frustrating. Effectively, your users are penalized for being secure. Well, if your org uses password management, your Salesforce for iOS users are free to leave the penalty box. With version 11.0 or later of Salesforce for Android and Salesforce for iOS, users can use a password manager app to simplify the login process down to a few taps.

Salesforce App Navigation Menu

Learn about the items that can appear in the navigation menu. You can customize most aspects of the navigation menu for your organization.

Salesforce App Notifications

Notifications let your users know when certain events occur in Salesforce. For example, notifications let users know when they receive approval requests or when someone mentions them in Chatter.

Work Offline with the Salesforce App

Your mobile users' productivity doesn't have to stop when there's no connectivity. When you enable caching and Offline Edit, users can keep working, unimpeded by a subway commute, FAA regulations, capricious cellular signals, or bunker-style buildings. Offline access is available for Salesforce for Android and Salesforce for iOS. The beta version of Offline Edit requires version 10.0 of Salesforce for Android or Salesforce for iOS.

Enable Visualforce Pages for the Salesforce App

You can use Visualforce to extend the Salesforce app and give your mobile users the functionality that they need while on the go. Before adding a Visualforce page to the Salesforce app, make sure the page is enabled for mobile use or it won't be available in the mobile apps.

Your Org's Branding in the Salesforce App

You can customize the Salesforce app to match some aspects of your company's branding, so the app is more recognizable to your mobile users. Custom branding is displayed in all versions of the Salesforce app.

Test Current Network Conditions from Salesforce for Android and Salesforce for iOS

Do your users ever ask why the Salesforce app is snappy in some locations but a little sluggish in others? Obviously the condition of a network can affect how Salesforce performs. If a user experiences issues with Salesforce for Android and Salesforce for iOS, version 10.0.2 or later, have him test his network so you can rule it out as the source of the problem.

What's Different or Not Available in the Salesforce App

The Salesforce app doesn't include all the functionality that's available in the full Salesforce site, whether your org is using Lightning Experience or Salesforce Classic. Learn about the Salesforce features that aren't available, that have functional gaps from what you're used to in the full site, or that work differently.

SEE ALSO:

Find Object Management Settings

Compact Layouts

Page Layouts

Customize Search Layouts

Salesforce App Setup Options

EDITIONS

Setup for the Salesforce app available in: both Salesforce Classic and Lightning Experience

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

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

See the many options for customizing the Salesforce app, to make it an effective on-the-go tool for your users' business needs.

All Salesforce app customization options are available from the Setup menu. For your convenience, you can access many settings pages more quickly from the Salesforce Mobile Quick Start setup page. In Salesforce Classic, from Setup, click **Salesforce Mobile Quick Start** (near the top of the Setup menu). In Lightning Experience, from Setup, enter *`Salesforce Mobile Quick Start`* in the `Quick Find` box, then select **Salesforce Mobile Quick Start**.

Note: We recommend using Google Chrome for the Salesforce Mobile Quick Start setup page. Microsoft Internet Explorer 9 or later and Mozilla Firefox are also supported.

Here are the Salesforce customization options you can consider for your organization.

- Do some basic setup using the Salesforce Mobile Wizard. From the Salesforce Mobile Quick Start page, click **Launch Quick Start Wizard**.
- Define the users who can access the Salesforce app.
  - For Salesforce for Android and Salesforce for iOS, from the Salesforce Mobile Quick Start page, click **App Security Controls**.
  - For mobile web, from the Salesforce Mobile Quick Start page, click **Mobile Browser Option**.
- Customize how data appears in the Salesforce app. Unless otherwise specified, you can access these customizations from the management settings for the object whose data you want to customize.
  - Optimize your page layouts so they display well on mobile devices. You can modify existing page layouts or create new, mobile-friendly page layouts. From the appropriate object management settings, go to Page Layouts.
  - Add expanded lookups, components (including the Twitter component), or Visualforce pages to the Mobile Cards section of a page layout to have them display as mobile cards. From the appropriate object management settings, go to Page Layouts.
  - Make sure that Visualforce pages are enabled for use, so they'll display in the app. From Setup, enter *`Visualforce Pages`* in the `Quick Find` box, then select **Visualforce Pages**. Click **Edit** next to the name of a page, and select `Available for Salesforce mobile apps`.
  - Define the fields that show up in an object's record highlight area and in related list preview cards by creating custom compact layouts. From the appropriate object management settings, go to Compact Layouts.
  - Verify that your existing search layouts populate search results with the desired fields. From the appropriate object management settings, go to Search Layouts.
- Make it easy and efficient to work in the field by creating actions that are tailored to your specific business activities and use cases.

  - Enable actions in the publisher for your organization. From Setup, enter `Chatter Settings` in the `Quick Find` box, then select **Chatter Settings**. Select the `Enable Actions in the Publisher` checkbox. (This option assumes that your organization has Chatter enabled and that you want the actions you create to display in the Chatter publisher. If your organization doesn't have Chatter enabled, you can still use actions but they only display in the Salesforce app and not in the full Salesforce site.)

    Note: If actions in the publisher aren't enabled, only standard Chatter actions (Post, File, Link, Poll, and Thanks) appear in the Chatter publisher in the full Salesforce site. When Chatter is enabled but actions in the publisher aren't, standard Chatter actions and nonstandard actions appear in the Salesforce app action bar and in third-party apps that use action lists. Nonstandard actions include Create, Update, Log a Call, custom actions, and Mobile Smart Actions.

  - Create global actions that allow users to add new object records with no automatic relationship to other records. From Setup, enter `Global Actions` in the `Quick Find` box, then select **Global Actions**. To customize the fields that are used by global actions, click **Layout** on the Global Actions page.

    Then add the new actions to the Mobile & Lightning Actions section of the global publisher layout so that they appear in the Salesforce app. From Setup, enter `Publisher Layouts` in the `Quick Find` box, then select **Publisher Layouts**.

  - Create object-specific actions that allow users to add new records or update data in existing records. From the management settings for the object that you want to add an action to, go to Buttons, Links, and Actions. To customize the fields used by an object-specific action, click **Layout** on the Buttons, Links, and Actions page.

    Then add the new actions to the Mobile & Lightning Actions section on the appropriate object page layout.

- Customize the options that are available in the Salesforce app navigation menu, and the order in which items appear. From the Salesforce Mobile Quick Start page, click **Navigation Menu**.
- Help keep Salesforce app users aware of important Salesforce activities by enabling in-app and push notifications. From the Salesforce Mobile Quick Start page, click **Notification Options**.
- Integrate third-party apps into the Salesforce app navigation menu by adding Lightning page tabs for the Lightning pages deployed to your organization. From Setup, enter `Tabs` in the `Quick Find` box, select **Tabs**, and then click **New** on the Lightning Page Tabs related list.
- Customize the Salesforce app to match the look and feel of your company's branding. From the Salesforce Mobile Quick Start page, click **Salesforce Branding**.
- Allow Salesforce for Android and Salesforce for iOS to automatically cache frequently accessed Salesforce data to secure, persistent storage, so users can view data when their devices are offline. (This option is turned on by default.) From the Salesforce Mobile Quick Start page, click **Offline Cache**.

You can also check out the *Salesforce App Admin Guide*, which walks you through using the Salesforce app declarative tools in Setup to get your organization ready for the Salesforce mobile experience.

Set Up the Salesforce App with the Salesforce Mobile Wizard

The Salesforce Mobile Wizard provides an easy way to complete the essential setup tasks. After you've set up Salesforce with this wizard, your sales reps can use Salesforce to run their business from their mobile devices.

Note: We recommend using Google Chrome for the Salesforce Mobile Wizard and the Salesforce Setup page. Microsoft Internet Explorer 9 or later and Mozilla Firefox are also supported.

If you're using Lightning Experience:

1. From Setup, click **Launch Wizard** in the Set Up Salesforce tile in the quick access carousel.

If you're using Salesforce Classic:

1. From Setup, click **Salesforce Mobile Quick Start**.
2. On the Salesforce Setup page, click **Launch Quick Start Wizard**.

Note: Although the Salesforce Mobile Wizard gets you up and running with basic setup tasks, it doesn't include all Salesforce app setup tasks. For example, although you can rearrange global quick actions via the wizard, the Salesforce app action bar and action menu can include other types of actions such as object-specific quick actions and standard Chatter actions, depending on the context.

After you've finished the wizard, you'll be directed to the Salesforce Mobile Quick Start setup page, which provides easy access to setup pages and documentation. For settings that are configured on a single page, the Quick Start page includes direct links to those pages. In cases where the settings are available on multiple pages in Setup, we've provided links to relevant documentation about the setting.

EDITIONS

Setup for the Salesforce app available in: both Salesforce Classic and Lightning Experience

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

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

USER PERMISSIONS

To use the Salesforce mobile wizard:

- Customize Application

SEE ALSO:

Put the Salesforce App In Your Users' Hands

Control Access to the Salesforce App

You can control your organization's access to Salesforce for Android and Salesforce for iOS and Salesforce mobile web.

Based on your organization's configuration, you can:

- Enable or disable access to Salesforce mobile web. From Setup, enter *`Settings`* in the `Quick Find` box, then select **Salesforce Settings**. See Enable the Salesforce Mobile Web.
- Control who can access Salesforce for Android and Salesforce for iOS, and configure other security policies. From Setup, enter *`Connected Apps`* in the `Quick Find` box, then select the option for managing connected apps. See User Access and Security Policies for Salesforce for Android and Salesforce for iOS.

EDITIONS

Setup for the Salesforce app available in: both Salesforce Classic and Lightning Experience

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

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

User Access and Security Policies for Salesforce for Android and Salesforce for iOS

Salesforce for Android and Salesforce for iOS are connected apps. As a result, you can control the users who have access to the apps, as well as other security policies. By default, all users in your organization can log in to Salesforce for Android and Salesforce for iOS.

You can control security and access policies for each of the Salesforce for Android and Salesforce for iOS, using settings components that are installed from the managed Salesforce connected apps package. These components need to be installed in Salesforce:

- Salesforce for Android
- Salesforce for iOS

These components are automatically installed when one of your users installs a Salesforce for Android and Salesforce for iOS from the App Store or Google Play on a mobile device and authenticates with your organization by logging in to the mobile app.

Alternatively, you can manually install the Salesforce and Chatter Apps connected apps package so you can review and modify the default security and access settings before rolling out the Salesforce for Android and Salesforce for iOS to your users.

When the Salesforce connected apps components are installed, they're added to the Connected Apps page. (From Setup, enter *Connected Apps* in the Quick Find box, then select the option for managing connected apps.) Here, you can view and edit the settings for each of the apps, including controlling user access with profiles, permissions, and IP range restrictions. An error message is displayed if a restricted user attempts to log in to a Salesforce for Android and Salesforce for iOS.

Push notifications for the Salesforce for Android and Salesforce for iOS aren't managed from the Connected Apps page. To manage these settings, from Setup, enter *Notifications* in the Quick Find box, then select **Salesforce Notifications**.

Offline access is enabled by default when one of the Salesforce for Android and Salesforce for iOS is installed. To manage these settings, from Setup, enter *Offline* in the Quick Find box, then select **Salesforce Offline**.

EDITIONS

Setup for the Salesforce app available in: both Salesforce Classic and Lightning Experience

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

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

USER PERMISSIONS

To edit your Salesforce for Android and Salesforce for iOS settings:

- Customize Application

To view your Salesforce for Android and Salesforce for iOS settings:

- View Setup and Configuration

SEE ALSO:

Salesforce Connected App Attributes

Connected Apps

Install a Connected App

Edit, Reconfigure, or Delete a Connected App in Salesforce Classic

Monitor Usage for an OAuth Connected App

Enable Salesforce App Notifications

Requirements for the Salesforce App

Salesforce Connected App Attributes

The following custom attributes are available for Salesforce for Android and Salesforce for iOS, which are also connected apps.

Several of the Salesforce app custom attributes have a default value that automatically applies when a user logs in to Salesforce for Android or Salesforce for iOS. If the default values are appropriate for your org, you're all set.

To change a default value, or configure an attribute that doesn't have a default setting, go to Setup in the full Salesforce site. Enter *Connected Apps* in the Quick Find box, select **Connected Apps**, then click **Salesforce for Android** or **Salesforce for iOS**. In the Custom Attributes section on the connected app page, click **New** and enter the attribute name and value.

Important: Remember to wrap attribute values in quotation marks.

Attribute Key	Attribute Value	Platform	Description
CALL_HISTORY	• DISABLED • ADMIN_DEFINED • SIMPLE	Android	• If set to DISABLED, removes call logging from the navigation menu. • If set to ADMIN_DEFINED, enables native Android call logging. • If set to SIMPLE, enables Aura call logging.
DISABLE_EXTERNAL_PASTE	• TRUE • FALSE	Android, iOS	• If set to TRUE, lets users copy and paste within the Salesforce app, but disables copying within and pasting outside of the Salesforce app. • If set to FALSE (default if attribute value isn't defined), lets users copy and paste within and outside of the Salesforce app.
FORCE_EMAIL _CLIENT_TO	The email app's URI scheme. Can differ by platform. For example, here's an Android URI	Android, iOS	If a user taps on an email action in the Salesforce app, the user is directed

EDITIONS

Setup for the Salesforce app available in: both Salesforce Classic and Lightning Experience

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

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

USER PERMISSIONS

To edit your Salesforce for Android and Salesforce for iOS settings:
- Customize Application

To view your Salesforce for Android and Salesforce for iOS settings:
- View Setup and Configuration

Attribute Key	Attribute Value	Platform	Description

	scheme example for Blue Mail, and an iOS URI scheme example for Gmail.
	Android:
	`https://play.google.com/store/apps/details?id=me.bluemail.mail&hl`
	iOS:
	`googlegmail:///co?to=`
			to the email app specified in the attribute value.
			You can specify one email app only.
			The attribute value you enter depends on the email app and the device platform.
			• For Android, use the URI listed in the Google Play Store for the desired email app.
			• For iOS, do an Internet search to locate the URI scheme for the desired email app. For example, search for *`iOS Mail URI scheme`*.

`SHOW_OPEN_IN`	• `TRUE` • `FALSE`	iOS	• If set to `TRUE`, lets users share a file from the Salesforce app via a link to the file, or open a Salesforce file in a third-party app. • If set to `FALSE`, disables users from sharing a file from the Salesforce app or opening a Salesforce file in a third-party app.
`SHOW_PRINT`	• `TRUE` • `FALSE`	iOS	• If set to `TRUE`, lets users print from the Salesforce app. • If set to `FALSE`, disables printing from the Salesforce app.

Tip: Connected app attribute changes take effect when users force quit the Salesforce app or when they log in to a new session. To ensure that new or modified settings take effect for all users, we recommend that you revoke access to the Salesforce app so everyone is required to log in again.

We also recommend that you warn users about the changes you intend to make, especially if you're going to restrict activities that were previously available. The Salesforce app doesn't display messages or indicators that connected app settings have changed.

SEE ALSO:

Edit, Reconfigure, or Delete a Connected App in Salesforce Classic

User Access and Security Policies for Salesforce for Android and Salesforce for iOS

Enable the Salesforce Mobile Web

You can control whether users can access Salesforce mobile web when they log in to Salesforce from a supported mobile browser. By default, mobile web is turned on for your organization.

Important: Use of the Salesforce Classic full site in a mobile browser isn't supported. While you can disable Salesforce mobile web for your organization, and individual users can turn off mobile web for themselves, regular use of the full site in a mobile browser isn't recommended. Your users may experience problems that Salesforce Customer Support won't investigate.

It's not possible to access the Lightning Experience full site from any mobile browser.

1. From Setup, enter `Settings` in the `Quick Find` box, then select **Salesforce Settings**.
2. Select `Enable the Salesforce mobile web` to allow all users in your organization to access the app. Deselect this option to turn off access to the app.
3. Click **Save**.

When this option is turned on, users who log in to Salesforce from a supported mobile browser are automatically directed to the Salesforce mobile web experience. Logging in from an unsupported mobile browser loads the Salesforce Classic full site, even when this option is selected.

In most cases, logging in from an unsupported mobile browser loads the Salesforce Classic full site, even if the `Enable the Salesforce mobile web` option is enabled. There are two exceptions for iPhone and iPad users, however. Users can access the mobile browser app from Google Chrome for iOS or the Gmail for iOS app's webview, but using the Salesforce app in these environments isn't supported.

SEE ALSO:

Turn Salesforce Mobile Web Off or On

Requirements for the Salesforce App

Update Personal Information

EDITIONS

Setup for the Salesforce app available in: both Salesforce Classic and Lightning Experience

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

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

USER PERMISSIONS

To view Salesforce mobile web settings:
- View Setup and Configuration

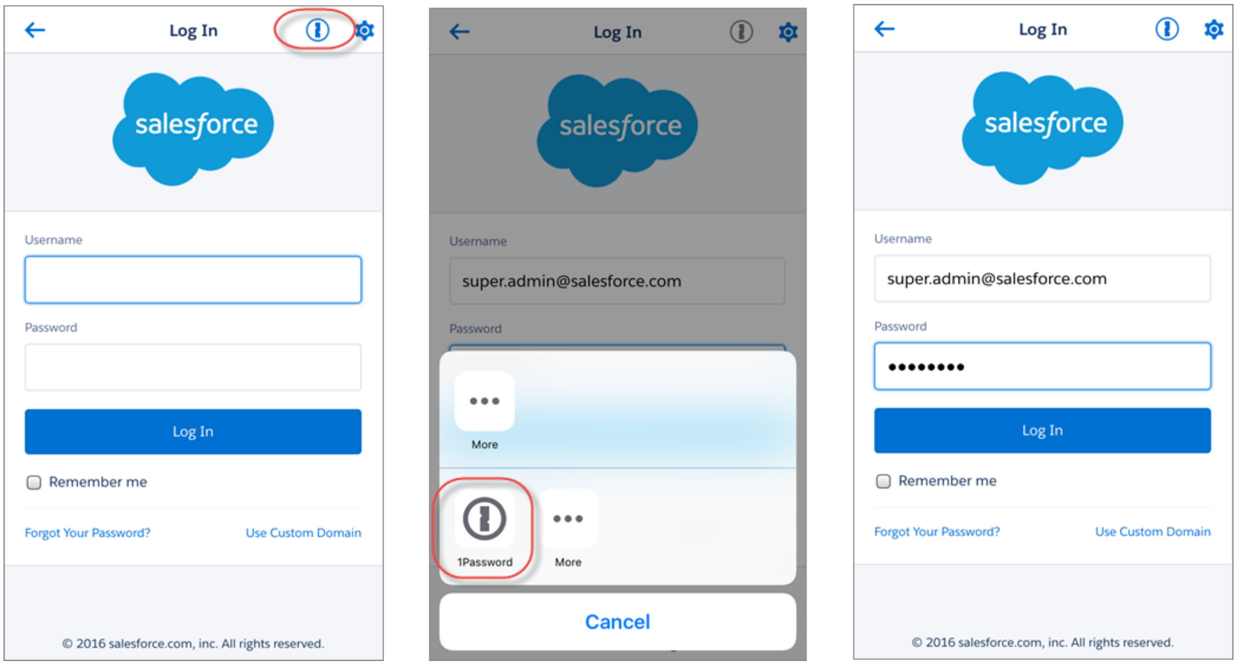
To modify Salesforce mobile web settings:
- Customize Application

  Modify All Data

Salesforce App and Password Manager Apps

Good security practices require long, complex passwords. But typing long, complex passwords on small mobile keyboards is error prone and frustrating. Effectively, your users are penalized for being secure. Well, if your org uses password management, your Salesforce for iOS users are free to leave the penalty box. With version 11.0 or later of Salesforce for Android and Salesforce for iOS, users can use a password manager app to simplify the login process down to a few taps.

Salesforce for iOS integrates with 1Password™, LastPass™, or other password manager apps that support the iOS password manager extension. After you set up password management for your org, Salesforce users simply tap ⓘ on the login page then select a password manager app from the list.



Username super.admin@salesforce.com

Password ••••••••

Salesforce App Navigation Menu

Learn about the items that can appear in the navigation menu. You can customize most aspects of the navigation menu for your organization.

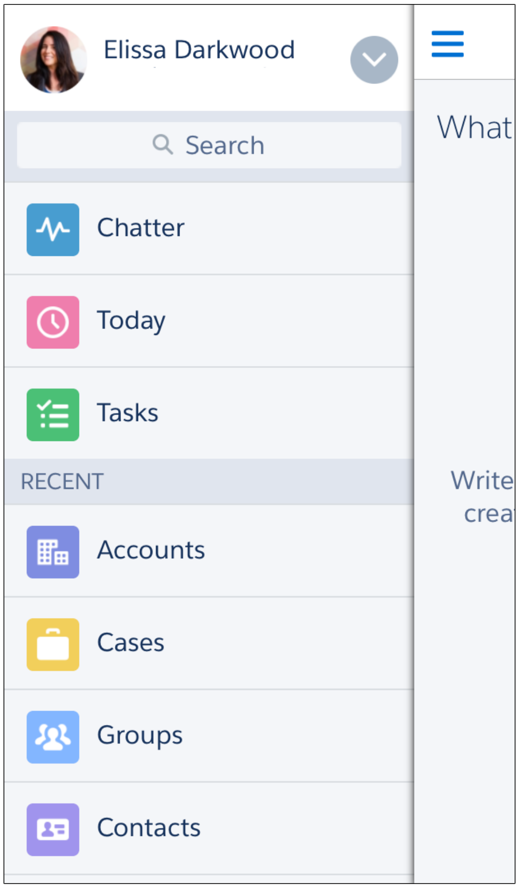
The ≡ icon in the header opens the navigation menu.

EDITIONS

Setup for the Salesforce app available in: both Salesforce Classic and Lightning Experience

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

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



If the default navigation menu doesn't meet your users' needs, you can easily customize it. From Setup, enter *`Navigation`* in the `Quick Find` box, then select **Salesforce Navigation**.

Depending on your organization's settings, the menu can contain:

Menu Item	Description
Approval Requests	Displays a list of the user's pending approvals. Users can tap an approval item and approve or reject it from within Salesforce. Available in Salesforce for iOS and mobile web.
Canvas apps	Appears for organizations that have enabled a canvas app to appear in the navigation menu.
Chatter	The user's main feed. Appears for organizations that have Chatter enabled.
Dashboards	Availability depends on edition and user permissions. If you don't add this item to the navigation menu, dashboards are automatically included in the set of Smart Search Items instead and the Dashboards item is available from the Recent section.
Events	Lists events owned by the user, that the user created for him- or herself, and that the user or a user's groups are invited to. If you don't add this item to the navigation menu, events are automatically included in the set of Smart Search Items instead and the Events item is available from the Recent section.

Menu Item	Description
Forecasts	Displays the Forecasts app, a helpful tool for every member of a sales team to keep track of forecast data and monitor progress towards quota. Available in the Salesforce for Android and Salesforce for iOS for iOS only. Note: Your org must have Collaborative Forecasts enabled. If your org uses Customizable Forecasts, the Forecasts item isn't available to add to the navigation menu.
Groups	Appears for organizations that have Chatter enabled. If you don't add this item to the navigation menu, groups are automatically included in the set of Smart Search Items instead and the Groups item is available from the Recent section.
Lightning component tabs	Only custom Lightning components that have a Lightning component tab associated with them can appear in the navigation menu.
Lightning pages	Custom app pages.
News	Displays the News app, a one-stop place for news and other insights about the user's accounts, contacts, leads, and opportunities.
Notes	Displays the Notes app. If you don't add this item to the navigation menu, notes are automatically included in the set of Smart Search Items instead and the Notes item is available from the Recent section.
Paused Flow Interviews	Displays a list of flow interviews that the user paused. An interview is a running instance of a flow. Users can tap an interview and resume or delete it. Available in Salesforce mobile web only.
People	Appears for organizations that have Chatter enabled. If you don't add this item to the navigation menu, profiles are automatically included in the set of Smart Search Items instead and the People item is available from the Recent section.
Reports	Availability depends on edition and user permissions. If you don't add this item to the navigation menu, reports are automatically included in the set of Smart Search Items instead and the Reports item is available from the Recent section.
Smart Search Items	Adds standard and custom Salesforce objects to the Recent section in the menu. This item also adds a set of the user's recently accessed objects to the Recent section and adds the More item so users can access all the objects they have permission to use and that are supported. If you don't include this item in the navigation menu, users can't access any objects on the navigation menu. Note: Smart Search Items is required for users to get search results in the Salesforce for Android and Salesforce for iOS for Android. Users of the Salesforce for Android and Salesforce for iOS for iOS and the Salesforce mobile web are able to search for records if this option is omitted from the navigation menu. If your iOS downloadable app users don't yet have a history of recent objects, they initially see a set of default objects in the Recent section. For Salesforce for Android and Salesforce mobile web, the default set of objects match the Lightning Experience Navigation Bar that the admin has configured in the Lightning App. If the user doesn't have access or permissions to the Lightning App, they also see a default set of objects until the user's most frequently used objects are determined. It can take up to 15 days for the objects that users work with regularly in both the Salesforce app and the full Salesforce site to appear in the Recent section. To make objects appear under Recent sooner, users can pin them from the search results screen in the full site.

Menu Item	Description
Tasks	Lists of a user's open and closed tasks and tasks that have been delegated. If you don't add this item to the navigation menu, tasks are automatically included in the set of Smart Search Items instead and the Tasks item is available from the Recent section.
Today	An app that helps users plan for and manage their day by integrating mobile calendar events with associated Salesforce tasks, accounts, and contacts. The app also allows users to instantly join conference calls, quickly log notes about events, and more. Available in the Salesforce for Android and Salesforce for iOS only.
Visualforce page tabs	Only Visualforce pages with the `Available for Lightning Experience, the Salesforce app, and Lightning Communities` checkbox selected will display in the Salesforce app.

Things to Keep in Mind

- You can't set different menu configurations for different types of users.
- Anything represented by a tab in Salesforce—such as standard and custom objects, Visualforce pages, the Chatter feed, People, or Groups—is visible for a user in the Salesforce app menu, based on the user's profile settings. For example, if a user is assigned to a profile that has the Groups tab set to Tab Hidden, the user won't see the Groups menu item in the Salesforce app, even though an administrator has included it in the menu.
- The navigation menu in a community isn't controlled via the Navigation Menu settings page. Instead, the tabs that are specified in Tabs & Pages in the community's administration settings determine the contents of the community's navigation menu.

SEE ALSO:

Customize the Salesforce App Navigation Menu

Notes About the Salesforce App Navigation Menu

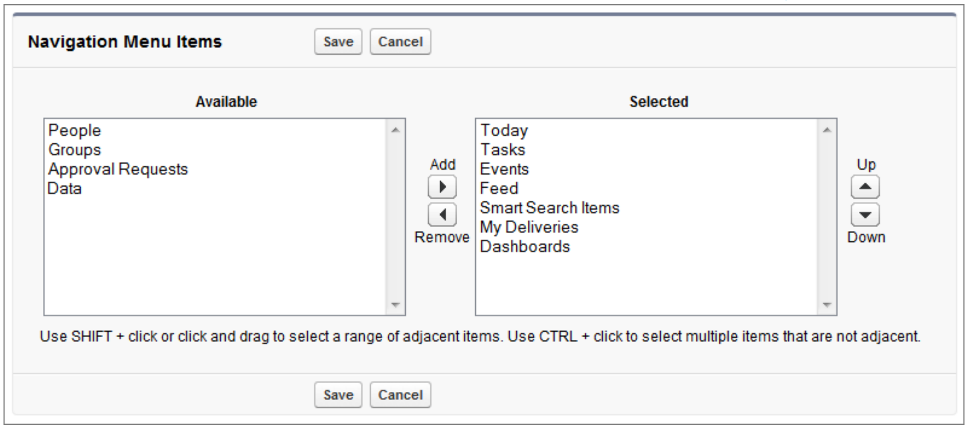
Enable Visualforce Pages for the Salesforce App

Customize the Salesforce App Navigation Menu

Customize your users' mobile Salesforce experience by selecting the menu items, apps, Visualforce pages, or Lightning pages to display in the Salesforce app navigation menu.

Note: Before you can include Visualforce pages, Lightning pages, or Lightning components in the Salesforce app navigation menu, create tabs for them. From Setup, enter *Tabs* in the `Quick Find` box, then select **Tabs**.

1. From Setup, enter *Navigation* in the `Quick Find` box, then select **Salesforce Navigation**
2. Select items in the Available list and click **Add**.


Navigation Menu Items Save Cancel

Available: People, Groups, Approval Requests, Data

Selected: Today, Tasks, Events, Feed, Smart Search Items, My Deliveries, Dashboards

Use SHIFT + click or click and drag to select a range of adjacent items. Use CTRL + click to select multiple items that are not adjacent.

3. Sort items by selecting them and clicking **Up** or **Down**.

   The order you put items in the Selected list is the order that they display in the navigation menu.

   Note: The first item in the Selected list becomes your users' Salesforce app landing page.

4. Click **Save**.

Once saved, the navigation menu items and their order should be reflected in Salesforce. You may need to refresh to see the changes.

Tip: When organizing the menu items, put the items that users will use most at the top. The Smart Search Items element can expand into a set of eight or more menu items and it might end up pushing other elements below the scroll point if you put it

EDITIONS

Setup for the Salesforce app available in: both Salesforce Classic and Lightning Experience

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

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

USER PERMISSIONS

To customize the Salesforce app navigation menu:
- Customize Application

near the top of the menu. Anything you put below the Smart Search Items element appears in the Apps section of the navigation menu.

SEE ALSO:

Salesforce App Navigation Menu

Notes About the Salesforce App Navigation Menu

Enable Visualforce Pages for the Salesforce App

Notes About the Salesforce App Navigation Menu

Some objects are excluded from the Recent section in the navigation menu, even if you accessed them recently.

- People, groups, notes, dashboards, reports, tasks, and events, if these items were added directly to the navigation menu
- List views, which are shown only on object home pages, not in the navigation menu
- Objects that aren't available in the Salesforce app, including any objects that don't have a tab in the full Salesforce site

About the Dashboards, Reports, Notes, Tasks, Events, Groups, and People Menu Items

If you opt to add the Dashboards, Reports, Notes, Tasks, Events, Groups, or People items to the Selected list for the navigation menu, these items appear in the order you specify, just like Today and other individual menu items.

If you don't add these items to the navigation menu, however, they're automatically included in the Smart Search Items set of objects and show up in the Recent section of the navigation menu.

EDITIONS

Setup for the Salesforce app available in: both Salesforce Classic and Lightning Experience

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

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

Pin an Object into the Recent Section

Users can customize the objects that appear in the Recent section of the navigation menu. If they search for an object in the full site, they can hover their mouse over the object name and click 📌 to pin it to the top of the search results. The order of pinned objects in the full site determines the order of the objects that stick to the top of the Recent section of the navigation menu. However, pinning objects in this way causes the unpinned objects remaining in the Recent section to drop into the **More** element.

Smart Search Items and Search Results in the Salesforce App

Smart Search Items adds standard and custom Salesforce objects to the Recent section of the navigation menu. Removing Smart Search Items from the navigation menu means users can't access objects (including object home pages and list views) from the menu.

Removing Smart Search Items also impacts search options. Because object home pages aren't available, it's not possible to run object-specific searches. The impact on global search depends on the Salesforce app.

- With Salesforce for iOS and Salesforce mobile web, users can find and access their records from global search results.

- Salesforce for Android requires Smart Search Items for global search to work. If Smart Search Items is omitted from the navigation menu, Android users can't locate records using global search.

SEE ALSO:

Salesforce App Navigation Menu

Customize the Salesforce App Navigation Menu

Salesforce App Notifications

EDITIONS

The Salesforce app available in: **All** editions except Database.com

Notifications let your users know when certain events occur in Salesforce. For example, notifications let users know when they receive approval requests or when someone mentions them in Chatter.

These types of notifications can appear to Salesforce app users.

- *In-app notifications* keep users aware of relevant activity while they're using the Salesforce app. By tapping 🔔, a user can view the 20 most recent notifications received within the last 90 days.

  If Salesforce Communities is enabled for your organization, users see notifications from all of the communities they're members of. To help users easily identify which community a notification came from, the community name is listed after the time stamp.

- *Push notifications* are alerts that appear on a mobile device when a user has installed the Salesforce for Android and Salesforce for iOS but isn't using it. These alerts can consist of text, icons, and sounds, depending on the device type. If an administrator enables push notifications for your organization, users can choose individually whether to receive push notifications on their devices.

Including Full Content in Push Notifications

Note: Some notifications include text that your users enter in Salesforce. To ensure that sensitive information isn't distributed through a third-party service without proper authorization, push notifications include minimal content (such as a user's name) unless you enable full content in push notifications.

For example, suppose an in-app notification reads: "Allison Wheeler mentioned you: @John Smith, heads-up! New sales strategy for Acme account." By default, the equivalent push notification would be "Allison Wheeler mentioned you." However, if you enabled full content in push notifications, this push notification would include the same (full) content as the in-app notification.

SEE ALSO:

Enable Salesforce App Notifications

Enable Salesforce App Notifications

Allow all users in your organization to receive mobile notifications about events in Salesforce, for example when they receive approval requests or when someone mentions them in Chatter.

1. From Setup, enter *`Notifications`* in the `Quick Find` box, then select **Salesforce Notifications**.
2. Select the notifications that you want your Salesforce app users to receive.
3. If you're authorized to do so for your company, select `Include full content in push notifications`.
4. Click **Save**.

   If you selected the option to include full content in push notifications, a pop-up appears displaying terms and conditions. If you click **OK**, you're agreeing to the terms and conditions on behalf of your company.

A user can receive approval requests in the Salesforce app notifications only when the user receives approval requests as email notifications. You or your user can change the `Receive Approval Request Emails` user field to set this preference.

SEE ALSO:

Salesforce App Notifications

EDITIONS

Setup for the Salesforce app available in: both Salesforce Classic and Lightning Experience

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

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

USER PERMISSIONS

To view notifications settings:
- View Setup and Configuration

To modify notifications settings:
- Customize Application

Work Offline with the Salesforce App

Your mobile users' productivity doesn't have to stop when there's no connectivity. When you enable caching and Offline Edit, users can keep working, unimpeded by a subway commute, FAA regulations, capricious cellular signals, or bunker-style buildings. Offline access is available for Salesforce for Android and Salesforce for iOS. The beta version of Offline Edit requires version 10.0 of Salesforce for Android or Salesforce for iOS.

Manage caching and Offline Edit from Setup—enter *`Offline`* in the `Quick Find` box, then select **Salesforce Offline**.

IN THIS SECTION:

Access Data in the Salesforce App While Offline

With caching in the Salesforce app enabled, your Salesforce for Android and Salesforce for iOS users can see important data when working offline or when the mobile app can't connect to Salesforce. The app caches a set of a user's recently accessed records so they're available for viewing without a connection. And much of the data that a user accesses throughout a Salesforce session is also added to the cache. Cached data is encrypted and stored in a secure, persistent data store.

Create, Edit, and Delete Records in the Salesforce App While Online or Offline (Beta)

Whether online or offline, Salesforce for Android and Salesforce for iOS users can create, edit and delete records and keep track of all of the changes from the Pending Changes page. The Salesforce app automatically syncs those pending changes to Salesforce and warns the user if there are conflicts that need to be resolved. The beta version of Offline Edit requires version 10.0 or later of Salesforce for Android or Salesforce for iOS.

Data and UI Elements That Are Available When the Salesforce App is Offline

With Salesforce app caching and Offline Edit, Salesforce for Android and Salesforce for iOS users can work with many of their frequently accessed objects and records while offline. Here's the list of data and Salesforce app user interface elements that are available offline.

Enable Offline Access and Edit for the Salesforce App

With just a few clicks, you can protect your Salesforce app users against the vagaries of mobile connectivity. You can enable two levels of offline access: caching frequently accessed records, so users can view data while offline, and Offline Edit, so users can create, edit, and delete records while offline. Offline access is available in the Salesforce for Android and Salesforce for iOS only. The beta version of Offline Edit is available in Salesforce for Android and Salesforce for iOS version 10.0 or later.

SEE ALSO:

Offline Access: What's Different or Not Available in the Salesforce App

Access Data in the Salesforce App While Offline

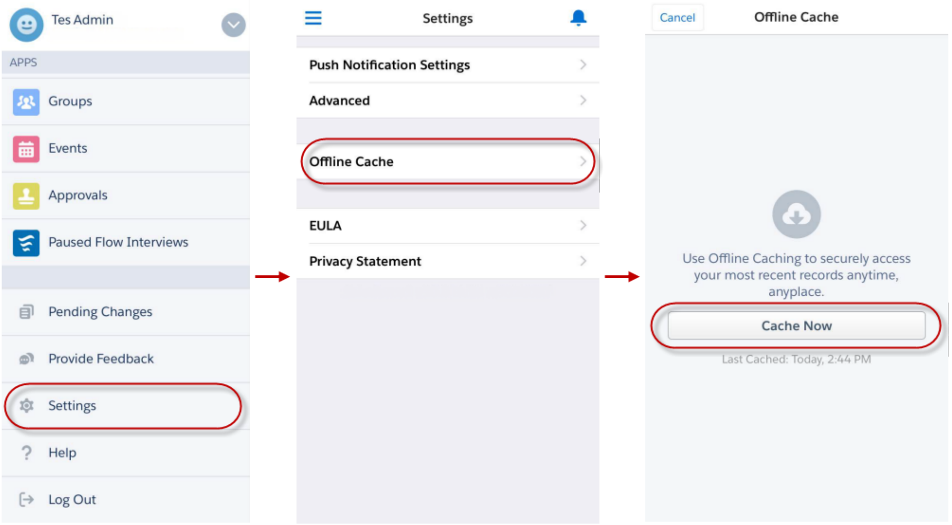
With caching in the Salesforce app enabled, your Salesforce for Android and Salesforce for iOS users can see important data when working offline or when the mobile app can't connect to Salesforce. The app caches a set of a user's recently accessed records so they're available for viewing without a connection. And much of the data that a user accesses throughout a Salesforce session is also added to the cache. Cached data is encrypted and stored in a secure, persistent data store.

Caching in the Salesforce app is enabled the first time someone in your org installs Salesforce for Android and Salesforce for iOS.

The contents of a user's cache determines the data that's accessible when the user's mobile device is offline. Let's look at how the cache is initially populated and then updated throughout a Salesforce app session.

Note: A session is the time between logging in to and out of the app. Putting the app in the background by switching away to a different app doesn't end a session.

- When a user logs in, the cache is empty. If the user's device goes offline with an empty cache, no Salesforce data is available.
- Users can quickly populate the cache with a default set of most recently accessed records in two ways. Users can put Salesforce in the background by switching away to a different app or navigating to the device home screen to populate their cache. Or users can go to the navigation menu, select **Settings** > **Offline Cache** > **Cache Now**.



Use Offline Caching to securely access your most recent records anytime, anyplace.

Last Cached: Today, 2:44 PM

Tip: We recommend that your users populate their cache each time they log in to Salesforce so they're guaranteed to have a meaningful set of available data when offline.

Depending on the size and complexity of a user's records, caching can take a few seconds to a couple of minutes. If the user goes offline before the cache is fully updated, some of the expected records won't be available.

Populating the cache collects recently accessed records for the first five objects listed in the Recent section of the user's navigation menu, plus the user's recent tasks and dashboards. For the first five objects listed in the Recent section of the navigation menu, up to 30 most recently accessed records are cached per object. For tasks and dashboards, the tasks listed under **My Tasks** and the five most recently accessed dashboards are cached. Recently accessed records are determined by a user's activities in both the app and the full Salesforce site, including Salesforce Classic and Lightning Experience.

After users initially populate their cache, users can refresh their cache in two ways. If the last cache refresh is more than one hour old, users can put Salesforce in the background by switching away to a different app or navigating to the device home screen to refresh the cache. Or users can manually refresh the cache by going to the navigation menu, select **Settings** > **Offline Cache** > **Cache Now**.

- Throughout a session, many of the other records that the user accesses are also added to the cache. (Not all Salesforce data is available offline—see Data and UI Elements That Are Available When the Salesforce App is Offline.)
- A record remains in the user's cache for 30 days. Each time the same record is accessed, the clock resets. But if the record isn't touched within 30 days, it's automatically removed from the cache and won't be available offline until the user accesses the record again.
- Logging out of Salesforce removes all data from the cache. The next time the user logs in, the process of generating the cache starts over.

SEE ALSO:

Data and UI Elements That Are Available When the Salesforce App is Offline

Enable Offline Access and Edit for the Salesforce App

Create, Edit, and Delete Records in the Salesforce App While Online or Offline (Beta)

Offline Access: What's Different or Not Available in the Salesforce App

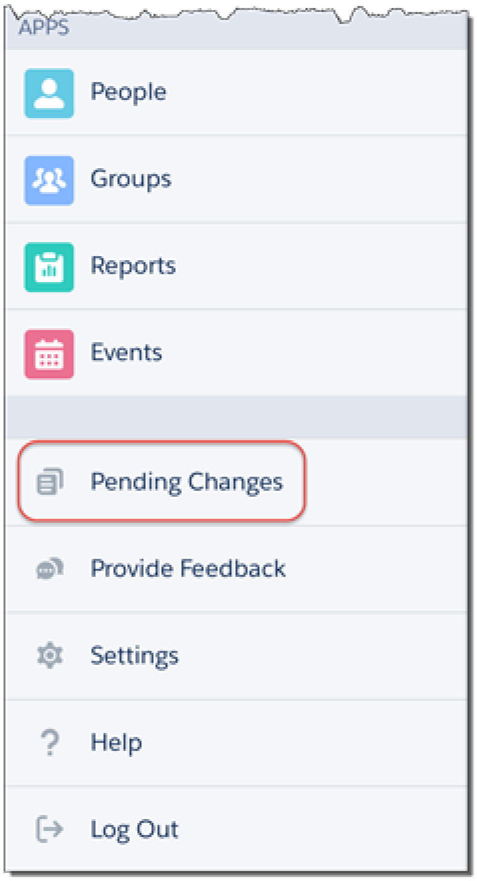
Create, Edit, and Delete Records in the Salesforce App While Online or Offline (Beta)

Whether online or offline, Salesforce for Android and Salesforce for iOS users can create, edit and delete records and keep track of all of the changes from the Pending Changes page. The Salesforce app automatically syncs those pending changes to Salesforce and warns the user if there are conflicts that need to be resolved. The beta version of Offline Edit requires version 10.0 or later of Salesforce for Android or Salesforce for iOS.

Note: This release contains a beta version of Offline Edit, which means it's a high-quality feature with known limitations. To enable this feature in your org, see Enable Offline Access and Edit for the Salesforce App. Offline Edit isn't generally available unless or until Salesforce announces its general availability in documentation or in press releases or public statements. We can't guarantee general availability within any particular time frame or at all. Make your purchase decisions only based on generally available products and features. You can provide feedback and suggestions for Offline Edit in the IdeaExchange in the Trailblazer Community.

Keep Track of Updates

Users can keep track of all changes made while online or offline from the Pending Changes page. This page is available from the Salesforce app navigation menu.



Understanding the Status of Updates

To help users monitor the status of changes made while online or offline, visual indicators display in several places in the Salesforce app, including: the Pending Changes page, object home pages, and in the highlights area on updated records.

- ◥: Indicates that there are no conflicts to changes made while online or offline. Records disappear from the Pending Changes page after successfully syncing to Salesforce.
- ◥: Indicates that there are conflicts to changes that must be resolved.
  - If the changes are made while online, the ◥ appears immediately to indicate that there are conflicts.
  - If the changes are made while offline, the ◥ appears when network connectivity is restored to indicate that there are conflicts.

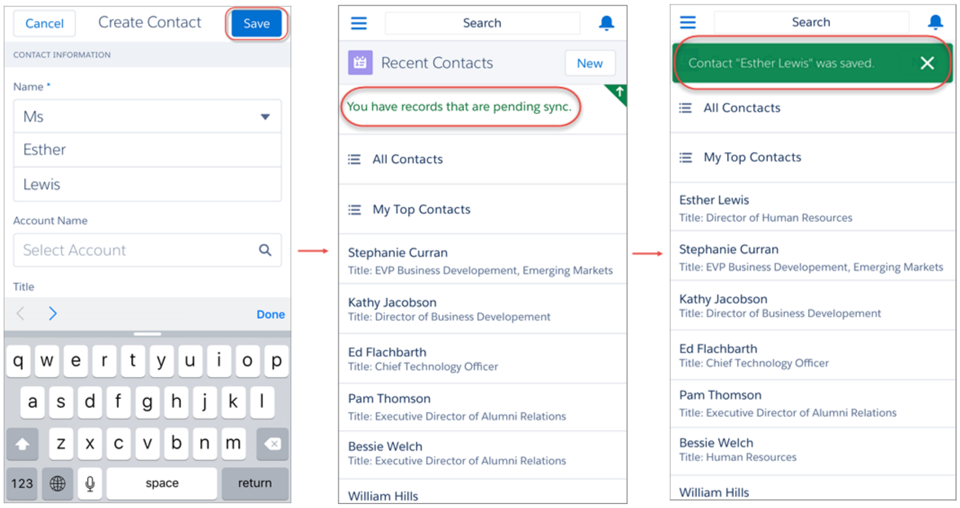
  Pending changes may contain conflicts for several reasons:
  - Validation rule error
  - Apex trigger error
  - Workflow rule error
  - Duplicate rule error

If users encounter conflicts when saving a record, whether online or offline, they must go to the Pending Changes page to see the details of the error. Users can tap on a record where ↑ appears, and they are taken to a Conflict Resolution page to resolve the issue. After the conflict is resolved, the record disappears from the Pending Changes page after successfully syncing to Salesforce.

- ⚠: Indicates that an error has occurred.
  - If the changes are made while online, the ⚠ appears immediately to indicate an error.
  - If the changes are made while offline, the ⚠ appears when network connectivity is restored to indicate an error.

When users tap on a record where ⚠ appears, they are taken to the edit page of that record to fix the error.

While rare in occurrence, sometimes an error is irreconcilable. For example, if an edit is made to a record while offline and someone else deleted that record from Salesforce, the ⚠ that appears on that change is irreconcilable. In this scenario, users can only dismiss the irreconcilable change from the Pending Changes page.



Ms
Esther
Lewis

You have records that are pending sync.

Stephanie Curran
Title: EVP Business Developement, Emerging Markets
Kathy Jacobson
Title: Director of Business Developement
Ed Flachbarth
Title: Chief Technology Officer
Pam Thomson
Title: Executive Director of Alumni Relations
Bessie Welch
Title: Executive Director of Alumni Relations
William Hills

Contact "Esther Lewis" was saved.

Esther Lewis
Title: Director of Human Resources
Stephanie Curran
Title: EVP Business Developement, Emerging Markets
Kathy Jacobson
Title: Director of Business Developement
Ed Flachbarth
Title: Chief Technology Officer
Pam Thomson
Title: Executive Director of Alumni Relations
Bessie Welch
Title: Human Resources
William Hills

See Data and UI Elements That Are Available When the Salesforce App is Offline for the full list of data that can be updated with Offline Edit.

SEE ALSO:

Data and UI Elements That Are Available When the Salesforce App is Offline

Enable Offline Access and Edit for the Salesforce App

Offline Access: What's Different or Not Available in the Salesforce App

Data and UI Elements That Are Available When the Salesforce App is Offline

With Salesforce app caching and Offline Edit, Salesforce for Android and Salesforce for iOS users can work with many of their frequently accessed objects and records while offline. Here's the list of data and Salesforce app user interface elements that are available offline.

Salesforce Data / Salesforce App Element	Available for Offline Viewing	Available to Create, Edit, or Delete Offline (Beta)
Navigation Menu	Yes	n/a
Action Bar	Yes	Edit action: Yes Delete action: Yes Other actions: No
Global Search	Previous search results from current session	n/a
List Views	If viewed in current session	No
Records for Recent Objects	Yes, recently accessed records for the first five objects (excluding Files) in the Recent section of the Salesforce app navigation menu	Yes, recently accessed records for the first five objects (excluding Files) in the Recent section of the Salesforce app navigation menu
Records for Other Objects	If viewed in current session	If viewed in current session
Related Records	If viewed in current session	If viewed in current session
Salesforce Today	Main page and mobile event records, if viewed in current session	No
Salesforce Events	If viewed in current session	Create: No Edit and Delete: If viewed in current session
Tasks	Most recently accessed tasks from the first page of My Tasks list only	Most recently accessed tasks from the first page of My Tasks list only (The simplified New Task form must be disabled)
Notes	If viewed in current session	Create: Yes Edit: If viewed in current session Delete: No
Files	If viewed in current session	No
Dashboards (Enhanced Charts)	Most recently accessed only	No
Dashboards (Legacy Charts)	No	No
Feeds, Groups, and People	If viewed in current session	No
Notifications	If viewed in current session	n/a
Approvals (submit, approve, or reject)	No	No
Visualforce pages	No	No
Canvas Apps	No	No
Lightning pages	No	No

Salesforce Data / Salesforce App Element	Available for Offline Viewing	Available to Create, Edit, or Delete Offline (Beta)
Salesforce App Settings	Yes	n/a

A Salesforce app session is the time between logging in and logging out of the app. Switching away from Salesforce app doesn't end the session as long as the user doesn't log out.

SEE ALSO:

Offline Access: What's Different or Not Available in the Salesforce App

Enable Offline Access and Edit for the Salesforce App

With just a few clicks, you can protect your Salesforce app users against the vagaries of mobile connectivity. You can enable two levels of offline access: caching frequently accessed records, so users can view data while offline, and Offline Edit, so users can create, edit, and delete records while offline. Offline access is available in the Salesforce for Android and Salesforce for iOS only. The beta version of Offline Edit is available in Salesforce for Android and Salesforce for iOS version 10.0 or later.

1. From Setup, enter *`Offline`* in the `Quick Find` box, then select **Salesforce Offline**.
2. To allow viewing data while offline, select `Enable caching in Salesforce for Android and iOS`.

   This option is automatically enabled the first time someone in your org installs either Salesforce for Android and Salesforce for iOS.
3. To allow updating records while offline, select `Enable offline create, edit, and delete in Salesforce for Android and iOS`.

   This option isn't available if caching in the Salesforce app is disabled.
4. Click **Save**.

Tip: We strongly recommend leaving `Enable caching in Salesforce for Android and iOS` enabled. In addition to making cached data available offline, this setting also enables faster viewing of previously-accessed records and better overall performance. If you disable caching, the Salesforce for Android and Salesforce for iOS only store the minimum data required to maintain a session. This can impact performance because the app has to refresh record details and feed items every time they're viewed.

SEE ALSO:

Work Offline with the Salesforce App

Offline Access: What's Different or Not Available in the Salesforce App

EDITIONS

Setup for the Salesforce app available in: both Salesforce Classic and Lightning Experience

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

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

USER PERMISSIONS

To view Salesforce app settings:
- View Setup and Configuration

To modify Salesforce app settings:
- Customize Application

  Modify All Data

Enable Visualforce Pages for the Salesforce App

You can use Visualforce to extend the Salesforce app and give your mobile users the functionality that they need while on the go. Before adding a Visualforce page to the Salesforce app, make sure the page is enabled for mobile use or it won't be available in the mobile apps.

Tip: Before exposing existing Visualforce pages in the Salesforce app, consider how they'll look and function on mobile phones and tablets. Most likely, you'll want to create a new page specifically for mobile form factors.

Visualforce pages must be enabled for mobile use before they can display in these areas of the Salesforce user interface:

- The navigation menu, via a Visualforce tab
- The action bar, via a custom action
- Mobile cards on a record's related information page
- Overridden standard buttons, or custom buttons and links
- Embedded in record detail page layouts
- Lightning pages

To enable a Visualforce page:

1. From Setup, enter `Visualforce Pages` in the `Quick Find` box, then select **Visualforce Pages**.
2. Click **Edit** for the desired Visualforce page.
3. Select `Available for Lightning Experience, Lightning Communities, and the mobile app` then click **Save**.

Consider these notes about Visualforce support.

- Standard tabs, custom object tabs, and list views that are overridden with a Visualforce page aren't supported. The Visualforce page is shown for full site users, but Salesforce app users will see the default Salesforce page for the object. This restriction exists to maintain the Salesforce app experience for objects.
- You can also enable Visualforce pages for the Salesforce app through the metadata API by editing the `isAvailableInTouch` field on the ApexPage object.
- The `Salesforce Mobile Classic Ready` checkbox on Visualforce Tab setup pages is for Salesforce Mobile Classic only and has no effect on Visualforce pages in the Salesforce app.

SEE ALSO:

Customize the Salesforce App Navigation Menu

Manage Mobile Cards in the Enhanced Page Layout Editor

Viewing and Editing Visualforce Pages

EDITIONS

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

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

USER PERMISSIONS

To enable the display of Visualforce in the Salesforce app:

- Customize Application
  Author Apex

Your Org's Branding in the Salesforce App

You can customize the Salesforce app to match some aspects of your company's branding, so the app is more recognizable to your mobile users. Custom branding is displayed in all versions of the Salesforce app.

EDITIONS

Setup for the Salesforce app available in: both Salesforce Classic and Lightning Experience

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

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

> Note: Images that you upload to customize the Salesforce app are stored in a Documents folder named Salesforce Branding Resources. For this reason, the Documents object must be enabled for your organization before administrators can view and modify the Salesforce app branding page. (The Documents tab doesn't need to be visible, however.)
>
> For users of Salesforce mobile web to see custom branding, Documents must be enabled for your organization. For Salesforce for Android and Salesforce for iOS, users must also have "Read" user permissions on Documents.

You can customize:

Element	Description
Brand Color	The color for key user interface elements such as the header, buttons, and search bar. Based on the brand color you select, contrasting colors for user interface elements such as borders for the navigation menu, the notifications list, and button text are automatically defined. The headers on overlays, popups, and dialogs—such as edit and create windows or windows that open from actions in the action bar—aren't affected by this setting. These headers are always white, to provide a visual indicator that the user is performing an action as opposed to simply viewing information.
Loading Page Color	The background color on the loading page that appears after a mobile user logs in.
Loading Page Logo	The image on the loading page that appears after a mobile user logs in. We recommend using an image with the largest dimensions allowable for best results. Maximum image size is 460 pixels by 560 pixels.

Consider the following tips when customizing the branding of the Salesforce app:

- When creating your logo image, be sure to compress it. In many image editing programs, this process is identified as "use compression," "optimize image," "save for web," or "shrink for the web."
- Verify that your logo appears correctly in Salesforce app, using the same devices as your user base, not just a desktop monitor. Your image can render at different scales or proportions depending on the screen size and pixel density of each device.
- The Salesforce app supports `.png`, `.gif`, and `.jpg` image formats for custom branding elements, but we recommend using .png for the best results.
- These interface elements can't be customized:
  - The Salesforce app icon that appears on the mobile device's home screen.

  - The initial loading screen when launching Salesforce for iOS. This loading screen appears before the user is prompted by the login page.
- Your mobile users must close the app and then log in again to see any custom branding changes.

You can also customize the branding for the Salesforce app login page. My Domain must be enabled to modify the login page. To customize your company's Salesforce app login page, see Customize Your My Domain Login Page with Your Brand on page 757.

SEE ALSO:

Customize Branding of the Salesforce App

Customize Branding of the Salesforce App

Change the Salesforce app's appearance, including the loading page background color, loading page logo, and header background color, so the app matches your company's branding.

Note: Images that you upload to customize the Salesforce app are stored in a Documents folder named Salesforce Branding Resources. For this reason, the Documents object must be enabled for your organization before administrators can view and modify the Salesforce app branding page. (The Documents tab doesn't need to be visible, however.)

For users of Salesforce mobile web to see custom branding, Documents must be enabled for your organization. For Salesforce for Android and Salesforce for iOS, users must also have "Read" user permissions on Documents.

1. From Setup, enter `Branding` in the `Quick Find` box, then select **fSalesforce Branding**, then click **Edit**.
2. To customize brand color for key user interface elements, including the header, click ▦ or enter a valid hexadecimal color code.
3. To customize the background color of the loading page, click ▦ or enter a valid hexadecimal color code.
4. To customize the loading page logo, click **Choose File** to upload an image. Images can be .jpg, .gif, or .png files up to 200 KB in size. The maximum image size is 460 pixels by 560 pixels.
5. Click **Save**.

SEE ALSO:

Your Org's Branding in the Salesforce App

EDITIONS

Setup for the Salesforce app available in: both Salesforce Classic and Lightning Experience

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

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

USER PERMISSIONS

To view Salesforce app branding settings:

- View Setup and Configuration

To modify Salesforce app branding settings:

- Customize Application

  Modify All Data

Test Current Network Conditions from Salesforce for Android and Salesforce for iOS

Do your users ever ask why the Salesforce app is snappy in some locations but a little sluggish in others? Obviously the condition of a network can affect how Salesforce performs. If a user experiences issues with Salesforce for Android and Salesforce for iOS, version 10.0.2 or later, have him test his network so you can rule it out as the source of the problem.

To test a network, open the navigation menu, then select **Settings** > **Test My Network**. From here, users can test ping, download speed, and upload speed.

EDITIONS

The Salesforce app available in: **All** editions except Database.com

This Test ...	Tells You ...
Ping	How long it takes for the app to send a request to Salesforce and then get a reply. In general, lower ping times are better than higher ones. If there's no result at all, the network may not be connected to the Internet. Results are reported in milliseconds.
Download Speed	How long it takes the app to get data from Salesforce. In general, higher download speeds are better than lower ones. Results are reported in bits per second.
Upload Speed	How long it takes the app to send data to Salesforce. In general, higher upload speeds are better than lower ones. Results are reported in bits per second.

If a test doesn't return a result, or an error is displayed, your user may be experiencing network connectivity issues that are affecting Salesforce. Ask the user to verify his Internet connection, and then run the test again. If the user continues to experience issues, ask him to try connecting to another network.

What's Different or Not Available in the Salesforce App

The Salesforce app doesn't include all the functionality that's available in the full Salesforce site, whether your org is using Lightning Experience or Salesforce Classic. Learn about the Salesforce features that aren't available, that have functional gaps from what you're used to in the full site, or that work differently.

- Data access and views
- Sales features
- Data quality and enhancement
- Productivity features
- Customer service features
- Reports and dashboards
- Salesforce Files
- Chatter
- Salesforce Communities
- Navigation and actions
- Search
- Entering data
- Approvals
- Offline access
- Salesforce customization

IN THIS SECTION:

Data Quality and Enhancement: What's Different or Not Available in the Salesforce App

SEE ALSO:

Locale and Language Support for the Salesforce App

Data Access and Views: What's Different or Not Available in the Salesforce App

Supported Objects and Data

These objects are available as items in the app navigation menu. You can create, view, and edit records for these objects unless noted otherwise.

- Accounts
- Assets
- Campaigns
- Cases
- Contacts
- Content Libraries *(iOS downloadable app only)*
- Contracts
- D&B Company *(view only, for Data.com Prospector and Data.com Clean customers)*
- Dashboards (*view only*)
- Events
- Files
- Field Service Lightning (Operating Hours, Service Appointments, Service Resources, Service Territories, Work Types) *(mobile browser app only)*
- Forecasts *(iOS downloadable app only)*
- Knowledge Articles (*view only*)
- Leads
- Live Chat Transcripts
- Opportunities
- Orders
- Quotes (*create from opportunities only*)
- Reports (*view only*)
- Social Personas and Social Posts
- Tasks
- Work.com Coaching, Goals, Thanks, Rewards, and Skills *(Skills not available in the iOS downloadable app)*
- Work Orders
- Custom objects that have a tab you can access
- Salesforce Connect external objects that are searchable and have a tab you can access

Note: To be available in the Salesforce app, an object must have a tab that you can access. This is true for supported standard objects and your org's custom and external objects.

The Salesforce app doesn't support the User object or provide access to user record detail pages. However, user fields are supported and appear on user profiles, in related lists, and so forth. See "Fields" for some issues with user fields.

The Salesforce app doesn't support:

- Standard or custom Salesforce apps. (Instead, the navigation menu gives users access to all of the objects that are available to them in the mobile app.)
- Salesforce Console or Agent Console.
- Advanced currency management.

Fields

Unsupported Fields

- division fields
- territory management fields

Combo Boxes

- Combo boxes, which combine a picklist with a text field, aren't available. Typically the text field is available but the picklist is not.

Lookup Fields

- User-defined lookup filter fields aren't supported.
- You can't create a record from a lookup field like you can in Lightning Experience.
- Lookup fields in Salesforce Classic show record names regardless of sharing permissions. As a result, users can see the names of records that they can't access. In Lightning Experience and the Salesforce app, lookup fields respect sharing permissions and only show the name of records that the user can access. The one exception is owner lookup fields, which always display the name of the record's owner, regardless of sharing permissions.

Picklist Fields

- Controlling and dependent picklists are supported, but doesn't display indicators on create and edit pages for these fields. To determine if a picklist field is dependent, and which picklist field controls it, switch to the full site.
- Disabled picklists aren't grayed out like they are in the full site.

Phone Number Fields

- The keypad that displays in phone number fields doesn't include parentheses, hyphens, or periods, and doesn't apply any phone number formatting when you save the record. To apply a specific phone number format, edit the record in the full site.

Rich Text Area Fields

Support for rich text area fields varies by the version of the Salesforce app and the type of device.

Device	App Version	View Rich Text Area Fields	Edit Rich Text Area Fields
Android	Salesforce for Android	Yes	Yes
	Mobile Web		The rich text editor isn't available. But you can manually add HTML tags.
iOS	Salesforce for iOS	Yes	Yes

Device	App Version	View Rich Text Area Fields	Edit Rich Text Area Fields
iOS	Mobile Web	Yes	Yes The rich text editor is available.
Windows	Mobile Web	No	No

User Fields

- While user detail pages aren't available in the app, user fields are supported and appear on user profiles, in related lists, and so forth.
- There are some issues when these user fields appear in related lists or mobile cards.
  - The `Company Name` field is blank if an internal user is viewing a mobile card or related list entry related to another internal user. If the referenced user is an external user, the company name appears correctly.
  - The `Active` field is blank unless the user is inactive.

List Views

- Creating list views or editing existing list views isn't supported.
- Editing a record's field in a list view isn't available. Instead, users can open the record then tap the **Edit** action.
- Selecting multiple records in list views isn't supported.
- Mass actions, which allow you to apply an action to multiple records at the same time, aren't available.

Record View and Record Highlights

- Customizations made to record highlights with Lightning App Builder, such as hiding fields or actions or displaying the highlights area vertically instead of horizontally, don't apply.
- Sections on the record detail page aren't collapsible.

Related Lists

- Related lists display the first four fields that are defined in the Related List section on an object's page layout. The number of fields shown can't be increased.
- Some related lists aren't available in the mobile app, including:
  - Content Deliveries
  - External Sharing
  - Related Content

  And see Sales Features in the Salesforce App, Productivity Features in the Salesforce App, and Customer Service Features in the Salesforce App for related lists that aren't available for specific objects.
- The Notes and Attachments related list isn't fully supported. There are several issues, including:
  - Attachments added in the full Salesforce site aren't guaranteed to open in the app, even if they appear in the related list. We recommend using Files instead. Documents that are uploaded to the Files tab in the full site are then viewable.

  - You can’t add or delete notes or attachments from the related list. (But you can create a note and relate it to a record, using the **Note** ( ) action in the action bar. Depending on how your administrator has configured Notes, this action may not be available for all objects.)
  - Notes and attachments on child records don’t display on the parent record’s related list.
- If a related list is sorted by a text area field, it doesn’t display any records.

Sales Features: What’s Different or Not Available in the Salesforce App

Accounts

- Automated Account Fields isn’t available, so when creating a new account, you won’t see suggested companies in the `Account Name` field.
- Social Accounts:
  - You can’t access social accounts features for Facebook, Klout, or YouTube.
  - If an account has been linked to a social network profile, the profile image selected for the account may display when viewing the account even when you aren’t logged in to the social network. Profile images from Facebook or Twitter may appear even if you aren’t currently logged in to those networks. You can’t switch to a different profile image.
  - You can view tweets, retweets, replies, or favorites for an associated Twitter user if you’re using Salesforce for Android or Salesforce for iOS. With mobile web, tap the Twitter profile to see tweets and so forth directly in Twitter. Also, in mobile web, you can’t see who is following a Twitter user, or who the Twitter user is following.
  - The Salesforce app lists common connections you and your account share on Twitter. You can’t view common connections in the full Salesforce site.
  - To view the Twitter card on accounts, you must add Twitter to the page layout. Access the full Salesforce site to edit page layouts. If your organization uses person accounts, the card must be added separately for business account layouts and person account layouts. The Twitter card is a separate component within the Related tab.
- The **Manage External Account** button isn't available.
- You can’t view the account hierarchy.
- You can’t merge accounts.
- You can view partners, notes, and attachments, but you can’t edit them.
- Accounts Home reports and tools aren't available.
- Records in the Contact Roles related list are read only. The Roles field on the Contact Roles related list isn’t available.
- You can’t clean account records with Data.com Clean.
- Person accounts can’t be edited or deleted from contact list views or contact related lists. Navigate to the person account record to edit or delete it.

Account Teams

- You can add, edit, or delete only one account team member at a time.
- When the account owner is changed, the account team is retained.
- Any user with edit access to an account can edit the account’s team members, but only changes to the Team Role field are saved.
- The **Display Access** button isn’t available.

Campaigns

- The **Manage Members** and **Advanced Setup** buttons aren't available.
- Campaign Hierarchy is available only as a related list. The option to **View Hierarchy** from a link on the campaign detail page isn't available. When viewing a parent campaign, the Campaign Hierarchy related list shows only the child campaigns, while the full site displays both the parent and child campaigns.
- When viewing the Campaign Members related list, only the members' Status appears. You can, however, tap members to see more details about them.

Contacts

- Contacts to Multiple Accounts:
  - Only the list item actions that are specific to the Account Contact Relationship object are available on the Related Accounts and Related Contacts related lists. Therefore, you see actions to view or remove the account-contact relationship, but not to edit or delete the contact or account record as you do in Salesforce Classic.
  - From the Related Contacts related list, you can navigate to a contact record, but not an account record.
- Social Contacts:
  - You can't access social contacts features for Facebook, Klout, or YouTube.
  - If a contact has been linked to a social network profile, the profile image selected for the contact may display when viewing the contact even when you aren't logged in to the social network. Profile images from Facebook or Twitter may appear even if you aren't currently logged in to those networks. You can't switch to a different profile image.
  - You can view tweets, retweets, replies, or favorites for an associated Twitter user if you're using Salesforce for Android or Salesforce for iOS. With Salesforce mobile web, tap the Twitter profile to see tweets and so forth directly in Twitter. Also, in Salesforce mobile web, you can't see who is following a Twitter user, or who the Twitter user is following.
  - The Salesforce app lists common connections you and your contact share on Twitter. You can't view common connections in the full Salesforce site.
  - To view the Twitter card on a contact, you must add Twitter to the page layout for contacts. Access the full Salesforce site to edit page layouts.
- You can't view the contact hierarchy.
- Activity logs aren't created when you use the ✉ icon to send emails.
- The **Request Update**, **Manage External User**, and **Enable Customer User** buttons aren't available.
- You can't add opportunities or account users on a contact, and you can't add a contact to a campaign.
- You can't merge contacts.
- You can't add contacts from Data.com or clean contact records with Data.com Clean.

Contracts

- Creating contact roles on contracts isn't available.

Einstein

- With the exception of lead scores appearing in lead list views, all other Sales Cloud Einstein features are unavailable in the mobile app.

Forecasts

- The Forecasts app is available in the Salesforce for Android and Salesforce for iOS for iOS, version 11.0 or later only.
- The Forecasts app requires Collaborative Forecasts. The app isn't available for orgs using Customizable Forecasts.
- Forecast data in is read-only.
- Only Opportunities - Revenue forecasts are available. These forecast types are not supported:
  - Opportunities - Quantity
  - Product Families - Revenue
  - Product Families - Quantity
  - Opportunity Splits - Revenue
  - Overlay Splits - Revenue
  - Custom Opportunity Currency Field - Revenue
  - Expected Revenue - Revenue
- Users can't change the forecasting currency.
- Showing and hiding quota information isn't supported.

Leads

- Social leads:
  - You can't access social leads features for Facebook, Klout, or YouTube.
  - If a lead has been linked to a social network profile, the profile image selected for the lead may display when viewing the lead even when you aren't logged in to the social network. Profile images from Facebook or Twitter may appear even if you aren't currently logged in to those networks. You can't switch to a different profile image.
  - You can view tweets, retweets, replies, or favorites for an associated Twitter user if you're using Salesforce for Android or Salesforce for iOS. With mobile web, tap the Twitter profile to see tweets and so forth directly in Twitter. Also, in mobile web, you can't see who is following a Twitter user, or who the Twitter user is following.
  - The Salesforce app lists common connections you and your lead share on Twitter. You can't view common connections in the full Salesforce site.
  - To view the Twitter card on a lead, you must add Twitter to the page layout for leads. Access the full Salesforce site to edit page layouts.
- Lead conversion:
  - You can select accounts but can't create them.
  - You can create opportunities but can't select existing ones.
  - You can't select lead sources across duplicate records. The lead source defaults to the duplicate contact.
  - You can't create related tasks during the conversion, but you can create tasks from the contact record.
  - You can't automatically notify owners of converted leads.
- The **Find Duplicates** and **Unlock Record** buttons aren't available.
- You can't merge leads.
- The Lead History related list isn't available.
- When adding a new lead, the `Campaign` field and the `Assign using active assignment rule" checkbox` aren't available. You can add values to these fields in the full Salesforce site.

News

- When accessing news from Salesforce on a smartphone, only one news item is displayed at a time.
- When accessing news from Salesforce on a tablet, you can't scroll through the available news items. Instead, the device's screen size determines the number of news items that are displayed.
- When navigating to other records, more news items can become available. It takes longer for those news items to appear in the News app.
- On account records, we don't include news cards for executives, which let you see a list of news items related to a single person. Instead, each news item that's related to an executive is shown on a separate news card.
- The News card is a separate component within the Related tab.

Opportunities

- The **Competitors** button isn't available.
- These fields aren't available: `Opportunity Splits` amount field, `Products` subtotal field, and `Stage History` connection field.
- Records in the Contact Roles related list are read only.

  The Roles field on the Contact Roles related list isn't available.
- The Campaign Influence and Similar Opportunities related lists aren't available.
- These related lists are available but the lists display record preview cards only; you can't tap to open any of the list records.
  - Competitors
  - Opportunity Splits
  - Stage History
- You can associate a price book with an opportunity that doesn't already have one, but you have to switch back to the full Salesforce site to change the association.
- You can't view product details, even for products that appear on the opportunity.
- You can add products with quantity or revenue schedules to an opportunity, but you can only edit product schedule in Salesforce Classic.

Opportunity Teams

- You can add, edit, or delete only one opportunity team member at a time.
- When the opportunity owner is changed, the opportunity team is retained.
- The **Clone** and **Display Access** buttons aren't available.

Orders

- You can't add or edit multiple products at the same time.
- You can't create reduction orders or select products to reduce.

Quotes

- Quote PDFs appear in the related list but aren't viewable.
- You can't add or edit multiple quote line items at the same time.
- You can't perform these actions.

  - Email quotes
  - Create or delete PDFs
  - Start sync or stop sync
  - Create quotes from the Quotes home page. You create quotes from opportunities.

Territory Management

- The original Territory Management feature isn't available.
- For Enterprise Territory Management users:
  - The Assigned Territories related list on accounts is read only, even for users with the Manage Territories permission.
  - The Users in Assigned Territories related list on accounts isn't available.

Productivity Features: What's Different or Not Available in the Salesforce App

Salesforce Today

The Salesforce Today app is available in the Salesforce for Android and Salesforce for iOS for Android phones and iPhone and iPad devices. It's not available in the Salesforce mobile web, nor in the full Salesforce site.

There are some issues when using Today.

- You see local events from selected calendars on your mobile device but Salesforce events aren't available in this release of Today.
- If some or all of your calendar servers don't automatically push data to your device, you need to update your calendars before you can see the most current information in Today.
- The 24-hour time format isn't supported.
- When viewing a multiday event, only the ending date and time are displayed in the highlights area.
- The wrong date and time may display for recurring multiday events.
- If your calendar doesn't display invitee names because the list is too long, Today shows a count of "1 invitee" in the Current Event and Agenda cards on the main view and doesn't show any invitees when you open the event.
- Today is unable to find a matching Salesforce record for a meeting organizer of an iCloud event because the iCloud API doesn't return an email address.
- Today uses the mobile device's time zone setting, while Salesforce events respect the user's Salesforce time zone setting. If there's a difference between these settings when a user logs a local event from Today, the `Time` field in the new Salesforce event record reflects the user's Salesforce time zone and doesn't match the time of the local event.
- On Android devices, a meeting organizer's name may not display correctly if there isn't a matching Salesforce record for the person.
- If another user makes updates to a mobile calendar event record while you're viewing the record in Today on an Android device, you don't automatically see the changes. The record is refreshed the next time you select it from the Today main view.
- Because of the way that the Android OS identifies local events, if a user accesses Today on an Android device to log a local event in Salesforce, then views the same event in Today on a different Android device or an iOS device, it may look like the event wasn't logged and it isn't possible to access the corresponding Salesforce event from Today. The logged event status and link is correct on the original Android device, however.
- Chatter Free and Chatter External users aren't able to access Today because these user license types don't have access to contacts or person accounts.

Activities (Events and Tasks)

- The activity timeline from Lightning Experience isn't available.
- The `Subject` field doesn't include a picklist of previously defined subjects.
- Activities can't be archived.
- You can't use Shared Activities to relate multiple contacts to an event or a task.
- Activity reminders aren't available.
- When an activity is related to a person account using only the `Name` field, the activity doesn't appear on the person account record.

Activities (Events and Calendars)

- You can't see a full calendar like you can in the full site. Nor can you create a calendar from standard or custom objects.
- You can't create a Microsoft® Outlook® appointment from a Salesforce event using the Add to Outlook button. However, if you're set up to sync events between Microsoft Office 365 and Salesforce using Lightning Sync, events you create and edit from Lightning Experience sync to Outlook automatically.
- Recurring events aren't available.
- Invitee related lists display slightly different content. In the Salesforce app, the invitee related list includes invitees only, whereas in the full site, it also includes the event owner. To reproduce the full site functionality, use an API query; see EventRelation.
- Event attendees in the Salesforce app require Lightning Sync with the sync direction Sync Both Ways and an account for Microsoft® Office 365® or Google G Suite. And event organizers have to create or edit their events from Lightning Experience, the Salesforce app, or their Microsoft or Google Calendar. Then organizers can view, invite, or remove contacts, leads, and other Salesforce users on their events. Event attendees can see contacts, leads, and other Salesforce users. Selecting Sync Both Ways limits some Salesforce Classic functionality. See Considerations for Syncing Events Between Microsoft® or Google Applications and Salesforce in Salesforce Help.
- To give reps access to attendees, add the Attendees field to the Event page layout for events. The Attendees field isn't supported for Compact Layouts.
- Attendees can see other attendees' responses from the Details tab in the Attendees field, but can't see responses from the related tab.
- Meeting attendees can't respond to event invitations from the Salesforce app. Users can accept or decline only from Microsoft Office 365 calendar or Google Calendar.
- Reps can't share calendars with coworkers or view coworkers' calendars.
- Events reflect your Salesforce time zone and locale settings, not the time zone setting on your mobile device.
- The date bar on the Events home page always begins on Sunday and ends on Saturday, regardless of your device and Salesforce locale settings.
- If you view the event list while the time advances from 11:59 PM to midnight, the list isn't automatically updated to display the next day's date and time.

Tasks

- Only the **My Tasks**, **Completed Within Last 7 Days**, **Delegated**, and **Today** lists are available. No other task lists, such as **Overdue**, **This Month**, or **All Open**, are available.
- In task lists, the order of the fields in the priority picklist determines the order in which tasks are sorted.
- The more tasks that you have, and the more relationships that your tasks have to other records, the longer it can take to view tasks or use other features.
- When more than 1,000 overdue tasks exist, task lists in the Salesforce app don't display any overdue tasks at all. Use reports to view your overdue tasks and close them, postpone them, or delete their due dates.

- Group (multiuser) tasks aren’t available.
- The `Create Recurring Series of Tasks` field isn’t supported on quick action layouts. Only a portion of the recurring task interface appears in new task quick actions, making it impossible for users to save any recurring tasks they attempt to create.
- You can’t create recurring tasks with a frequency of every weekday. And we don’t recommend editing tasks with this frequency because the edit page doesn’t show the task’s recurrence settings. To create or edit tasks that repeat every weekday, use Salesforce Classic.
- If a task doesn’t include a subject, it appears in feeds as [No Subject].
- The All Activity History tab isn’t available.
- Notifications for task reminders aren’t delivered as push notifications, so reps don’t see a notification or popup on their mobile device’s lock screen. Instead, reps get reminders in the notifications tray.
- Reps can’t create a task with a reminder unless you turn off the **Show simpler New Task form on mobile** setting. From Setup, enter *`Activity Settings`* in the Quick Find box, then select **Activity Settings**. Deselect **Show simpler New Task form on mobile**.
- Task layouts contain a few unique elements that make tasks easier to work with. These elements don’t appear in a compact layout because you can’t change them, but users always see them:
  - The □ and ☑ icons represent the status of the `IsClosed` field to users with the Edit Task permission.
  - The 🚩 icon represents a task marked high priority (including custom high priority).
  - If the due date exists and a user has permission to view it, all tasks show the due date.
  - Tasks include the primary contact and the related account or other record, when they exist.

  The fields in each list can vary depending on the settings in your Salesforce org.

  You control the layout of task records and tasks in the task list using compact layouts. You control related lists, as always, using the page layout editor. Adding the due date field to either layout doesn’t change the appearance of tasks—that field never appears twice.

  Below the built-in task elements, the Salesforce app displays up to three other fields.

  - The default compact layout for tasks includes two fields: the name of a lead or contact, and an opportunity, account, or other record the task is related to.
  - In an Activities related list, a task’s fields depend on what record you’re viewing and how you’ve defined the layout for that object.

  For more information, see Compact Layouts.

Notes

- You can access all your notes from the **Notes** item in the navigation menu. The Salesforce Classic version of the full site doesn’t include a Notes tab. Instead, Salesforce Classic users access notes from the **Files** tab.
- You can’t share notes with other users or groups.
- In Salesforce for Android and Salesforce mobile web, you can’t add images to notes, but you can view images that were added from the full site. You can, however, add images to notes using Salesforce for iOS, version 10.0 or later.
- Some rich text options that are available in the full site, such as applying a bold or italic font or indenting a paragraph, aren’t available. But you can view formatting that was added from the full site.
- You can’t revert to previous versions of notes, but you can view previous versions.
- Spelling errors aren’t highlighted while creating or editing notes.

Email

- The app doesn't display emails in the improved layout that's available in Lightning Experience.
- Inbox isn't available.
- List email is not available. However, users can see completed list email activities in the activity timeline.

Dialer

- The telephony features in Lightning Experience aren't available.
- Skype for Salesforce isn't available.

Work.com

When using Work.com features, you can't:

- Share goals and metrics
- Link metrics to reports
- Refresh metrics that are linked to reports
- Link parent goals and subgoals
- Add goal images
- Create custom badges
- Offer or request feedback
- View custom metric fields
- Create, fill out, or dismiss performance summaries
- Manage performance summary cycles

Data Quality and Enhancement: What's Different or Not Available in the Salesforce App

Duplicate Management

The Salesforce app doesn't alert users to existing duplicate records, either on the same object or across accounts, contacts, and leads.

For existing records:

- The app doesn't alert users to existing duplicate accounts, contacts, or leads.
- Merging of duplicate records isn't supported.

For new records:

- The app alerts users when they're about to create an account, contact, or lead that appears to duplicate an existing record.
- Each possible duplicate is shown on a "duplicate card." The app displays a maximum of 30 duplicates (10 per object), even if there are more.
- A duplicate card displays three fields, which are derived from the search results format defined for your org, not from the associated matching rule.
- If you tap a duplicate card that appears while you're editing or creating a record, any information you've entered is lost.
- By default, duplicate rules run when you complete fields on a record, rather than when you save a record.

Data Assessment for AppExchange Package Data

Data Assessment for data in AppExchange packages isn't available.

Account Data Assessment

Account Data Assessment (based on the Data.com Company Info for Accounts rule) isn't available.

Data Integration

You can see fields that were updated by data integration rules, but you can't use Data Integration to manually update records.

Data.com Clean

You can see fields updated by Clean jobs, but the option to manually clean records isn't available.

Data.com Prospector

Data.com Prospector isn't supported in the Salesforce app. You can't search for or add accounts, contacts, or leads. Nor can you see Prospecting Insights or Company Hierarchy.

Customer Service Features: What's Different or Not Available in the Salesforce App

Cases and Case Feed

- For organizations that have the legacy "Page Layouts for Case Feed Users" enabled, users who are assigned the "Use Case Feed" permission see the standard case layout.
- Standard actions on Case Feed aren't available. But several actions that duplicate this functionality are available. Salesforce admins can add these actions to the Mobile & Lightning Actions section on case page layout so they're available from the action bar when working with cases.

Standard Action Available in Salesforce Classic	Equivalent Action for the Salesforce App
Email	Send Email
Change Case Status	Update Case
Log a Call	Log a Call

  The **Portal** action isn't available.

- There are some differences in behavior when using case Send Email actions.
  - The `CC` and `BCC` fields on the Send Email publisher aren't collapsible.
  - HTML isn't supported in Send Email actions on cases. If a Send Email action includes an `HTML Body` field, html markup tags don't appear in the Send Email publisher or in emails created from the action.
  - It's not possible to include email attachments when using a case Send Email action.
  - If a default email template is assigned to a case Send Email action, any attachments included in the template are ignored. The attachments don't appear in the Send Email publisher and aren't included in emails created from the action.
- The Milestone component for cases, including the tracker, isn't displayed.
- You can't create, edit, or delete case comments. Also, the Case Comments related list doesn't display the full text of comments that were added in the full site.
- These case related lists aren't available:
  - Business Hours on Holiday List
  - Case Contact Role
  - Solution List
  - Team Member List
  - Team Member on Team List
  - Team Template Member List

Field Service Lightning

- When you create a record from a field service related list, the field that lists the parent record doesn't populate until you save the record. This issue applies to all versions of the Salesforce app. For example, when you create a service appointment from the Service Appointments related list on a work order, the `Parent Record` field is blank until you tap **Save**. Once the record is created, the parent record field lists the parent work order as expected.
- You can't create a service report, to create a service report, use the Field Service Lightning mobile app.
- The dispatcher console, which is part of the Field Service Lightning managed packages and includes the service list, scheduling policy picker, Gantt view, and map, isn't available.

Salesforce Knowledge Articles

Articles are supported in the Salesforce for Android and Salesforce for iOS for iOS, version 10.0 or later, the Salesforce for Android and Salesforce for iOS for Android, version 8.0 or later, and in the Salesforce mobile web, with these limitations:

Issue	Android Downloadable App, v8.0 or later	iOS Downloadable App, v10.0 or later	Mobile Browser App
Only published articles are available—not draft or archived articles.	🟥	🟥	🟥
Articles can't be created, edited, translated, or archived.	🟥	🟥	🟥
Articles can't be linked to cases. (But links that are set up from the full site can be viewed on the Related tab.)	🟥	🟥	🟥
Smart links aren't supported.	🟥	🟥	🟥
Article ratings aren't supported.	🟥	🟥	🟥
Tables are sometimes cut off on the right side when included in article rich text fields.	🟥		🟥
Compact layouts display the article type API name instead of the article type name. So users see the article type API name in the highlights area when viewing an article.	🟥	🟥	
When searching from the Articles home page, only articles in the user's language are returned and only if that language is an active Knowledge language (from Setup, **Customize** > **Knowledge** > **Knowledge Settings**). To see articles in another language, users can change to an active Knowledge language. From **My Settings**, use the Quick Find search box to locate the Language & Time Zone page.	🟥	🟥	
In global search, search results show articles in the language specified for the device, regardless of the active Knowledge language.	🟥		
Filtering search results by data categories, article type, validation status, or language isn't available.	🟥	🟥	🟥
In global search, articles don't appear in the list of recent records.	🟥	🟥	
In global search results, search highlights and snippets don't appear.	🟥	🟥	

Issue	Android Downloadable App, v8.0 or later	iOS Downloadable App, v10.0 or later	Mobile Browser App
These features are available in all versions of the Salesforce app when searching from the Articles home page.			
Knowledge articles aren't available when accessing communities via the Salesforce app.	🟥	🟥	

Social Customer Service

- To reply to social posts, you must use Salesforce Classic.
- Moderation and authorization pages aren't available.

Work Order Milestones

- The milestone tracker isn't available.
- Entitlement processes and milestones must be managed from the full Salesforce site.

Work Orders and Linked Articles

- Linked articles are view-only. You can search the Knowledge base and read attached articles, but you can't attach or detach articles. To manage linked article settings and attach or detach articles, use the full site.
- The Linked Work Orders and Linked Work Order Line Items related lists on articles aren't available.
- Linked articles can't be accessed from feed items.

Reports and Dashboards: What's Different or Not Available in the Salesforce App

Reports

Considerations When Using Reports in the Salesforce App

Feature	Notes about Salesforce App Availability
Number of Rows Displayed	Reports display a maximum of 2,000 rows, same as on the full Salesforce site.
Groupings	When you view a report with groupings, the groupings are displayed as columns at the end of the report.
Report Formats	Summary reports, matrix reports, and tabular reports are available, but matrix and summary reports are shown in tabular format. Joined reports aren't available.
Conditional Highlighting	You can't view reports that show conditional highlighting.

Feature	Notes about Salesforce App Availability
Filters	When you open a report from the Reports tab, you can't filter the report. When you tap a dashboard component to open the source report, you can filter the report by tapping a value on the chart. If the source report is a tabular or joined report, then you can’t filter it.

Report Features Not Available

- Create, edit, or delete reports
- Export
- Print
- Feed
- Schedule report refreshes
- Subscribe
- Joined reports
- Historical trend reports
- Add to campaign
- Role hierarchy
- Custom summary formula fields
- Folders
- Hide details
- Summary information (grand totals, subtotals, summarized fields, record counts, etc.)

Other Notes about Using Reports

- You can’t drill into reports that have more than three checkbox fields.
- When you view a report with more than 16 summary fields, you receive an error message.
- The Salesforce app can’t render reports via URLs that use dynamic parameter values. If you modify a URL to pass parameters into reports, the app shows a blank screen (a report record with no returned results).

Dashboards

Considerations When Using Dashboards

Feature	Notes about Salesforce App Availability
Edit a Dashboard	You can’t edit dashboards. Dashboards are read-only.
View As	As in the full Salesforce site, you can only run dashboards as a user in your role hierarchy. However, in the Salesforce app you can choose from all users in your organization. If you select a user outside your role hierarchy, you get an error.

Feature	Notes about Salesforce App Availability
Dashboard Layout	With Enhanced Charts, dashboards display in a single-column layout on phones, and up to a two-column layout on tablets. With Classic Charts, Lightning Experience dashboards that have more than three columns display in a three-column layout on phones and tablets.

Dashboards Features Not Available

- Create, edit, or delete dashboards
- Feed
- Schedule
- Link from a dashboard component to a website or email address
- Visualforce components on dashboards
- Folders

Other Notes about Using Dashboards

In some situations, data displayed in a dashboard component can get out of sync with data in the report that's displayed on the same page. When a dashboard component's data doesn't match the report, one of these things is happening:

- The dashboard is being refreshed as the configured user or the running user, while a report is always run as the current user.
- The report was refreshed more recently than the dashboard. A report is refreshed every time you look at it (assuming you aren't working offline). But a dashboard component is refreshed only when the dashboard it belongs to is refreshed.

The same temporary mismatch can occur in the full site, but there you see reports and dashboard charts on separate pages. You see the report and the dashboard chart on the same page.

Charts

Other Notes about Using Charts

- Unless you turn on **Enable Enhanced Charts in Salesforce**, legacy Salesforce Classic Charts display instead of the new Lightning Experience Charts. After turning on **Enable Enhanced Charts in Salesforce**, all users see Enhanced Charts regardless of whether they switch to Lightning Experience on the full Salesforce site.

  Enhanced Charts are similar to Legacy Charts, but there are a few differences:

  - Except for line and bar charts, which display up to 500 groups, Enhanced Charts show only the first 200 groups.
  - On tablets, dashboards always have two columns. On phones, dashboards always have one column.
  - On mobile dashboards, Enhanced Chart components don't show footers, but titles and subtitles still display. If there is important information in a component footer, consider moving it to the title or subtitle.
  - You can't share metric, gauge, or table charts in Chatter.
  - Enhanced Charts have a different color palette than Legacy Charts.

  Note: If your org was created during or after the Summer '16 release, then Enhanced Charts are turned on by default and Legacy Charts aren't available. In Spring '18, in all orgs, the Salesforce app will feature Enhanced Charts only because Legacy Charts are being retired.

- Report Charts are only available after drilling into a dashboard component's report. Report charts aren't available from the Reports tab.

- Embedded report charts don't link to the source report.

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

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

When using Salesforce Files in the Salesforce app, you can't:

- 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
- 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 full 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
  - 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.
- Interacting with content packs in is limited. Users can see the content packs that exist and share them with Salesforce colleagues or groups. But it's not possible to preview or download the files included in a content pack. Nor can mobile users create or modify content packs.

- Creating or managing content deliveries isn't available. This includes generating an encrypted URL for sharing files and content packs with customers.

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

Feeds

When viewing feed items in the Salesforce app, you can't see:

- Live feed or live comment updates.
- Rich text formatting or code snippets in the main feed. (*Salesforce for Android and Salesforce for iOS only*)
- Inline images in the main feed—you see a placeholder with the name of the image instead. (*Salesforce for Android and Salesforce for iOS only*)
- Multiple attachments on an item in the main feed—only the first attachment is displayed. (*Salesforce for Android and Salesforce for iOS only*)
- Previews of links in the main feed. (*Salesforce for Android and Salesforce for iOS only*)
- The list of people who liked a post. (*Salesforce mobile web only*)
- Bundled posts in the What I Follow feed. (*Salesforce for Android and Salesforce for iOS only*)
- Social feed posts. (*Salesforce for Android and Salesforce for iOS only*)
- The full content of posts shared from Lightning Experience when viewed in the main Chatter feed (*Salesforce for Android and Salesforce for iOS only*) or in feeds on profiles (*Salesforce for iOS only*). Tap the **View Post** link in the shared feed item to see the shared content.

When posting, commenting, or doing other work in feeds from the Salesforce app, you can't:

- Apply rich text formatting or include code snippets in feed items.
- Use Chatter emoticons (but you can use iOS and Android emoji keyboards to add emoticons to feeds).
- Add inline images to feed items.
- Add more than one attachment to feed items.
- Edit feed posts or comments.
- Mute a feed item. (*downloadable apps only*)
- Use action links in the main feed. (*downloadable apps only*)
- Share posts. (*mobile browser app only*)
- Search in feeds on user profiles and records.

There are some other features that aren't available from in Chatter. You can't:

- Switch the main feed to show only muted posts.
- Filter the main feed to show all updates, fewer updates, questions, or only posts related to a specific object.
- Send or view Chatter messages.
- See recommendations.
- Add or view Chatter favorites.
- See Chatter activity statistics or Chatter influence status.
- Invite coworkers to sign up for Chatter.

Topics

Topics are available in Salesforce mobile web, Salesforce for Android, and Salesforce for iOS. When using topics, you can't:

- See trending topics.
- Edit topic details (name and description).
- Tag favorite topics.
- Assign topics to records.
- View records assigned to a topic.
- See these related lists: Related Topics, Related Groups, Knowledgeable on Topics, Recent Files.
- See topics in auto-complete options when searching.
- Delete topics.
- Access the topic detail page by tapping on a hashtag topic from a feed (on Android devices).

Chatter Questions

When using Chatter Questions, you can't:

- See similar questions and knowledge articles when you ask questions.
- Select best answers.

Note: Chatter Questions isn't fully supported in Salesforce for Android and Salesforce for iOS. When coworkers ask questions, you can see who posted but the text of the question isn't displayed. You can see any answers to the question, however.

Groups

When using groups, you can't:

- See live feed updates.
- Use the group creation wizard to set up a new group.
- See recommendations of groups to join.
- Invite customers to join private customer groups.
- Add records to Chatter groups with customers using the **Add Record** action.
- Withdraw requests to join private groups.
- Change email and in-app notification settings for groups in communities.
- See or customize group member engagement data.

Group owners and managers can't remove files from the group files list.

People and Profiles

When using People to view profiles, you can't:

- Edit profile information in Salesforce for iOS .
- Upload a profile photo using the Good Access™ secure mobile browser.
- Hover on user profile photos to quickly see user information.
- Use custom profiles.
- Filter the Following related list on your profile.

Chatter Messenger

Chatter Messenger isn't available.

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

Salesforce Communities in the Salesforce app is similar to the full site, with these differences:

- The navigation menu for a community doesn't include all the items that are available to your internal organization:
  - The navigation menu shows only the tabs that the admin has included in that community via Tabs & Pages in the community's administration settings.
  - The Chatter tab that's available in Salesforce Classic is divided into three menu options in the Salesforce app (and Lightning Experience). If your community includes the Chatter tab in Salesforce Classic, you see Feed, People, and Groups in the Salesforce app.
  - The Events and Today items aren't available and don't appear in the navigation menu.
  - Tasks are available only to users with the Edit Tasks permission.
  - The Reports item isn't available and doesn't appear in the navigation menu.
  - Salesforce Knowledge articles aren't supported in communities when using the Salesforce for Android and Salesforce for iOS. The Articles item doesn't display in the navigation menu. (But articles are available if using the Salesforce mobile web.)
- There is no All Company nor Company Highlights feed.
- Adding inline images to a post isn't available.
- Community Management and Community Workspaces aren't available.
- Communities that use a Community Builder template, such as Koa, Kokua, or Customer Service (Napili), contain rich styling that doesn't display. These communities are responsive and it's best to access them directly from a mobile browser using community URLs. (Communities that use a Salesforce Tabs + Visualforce template *are* supported in all the Salesforce app.)
- Site.com branding is not supported.
- Community members can't flag private messages as inappropriate.
- Reputation isn't supported. However, if reputation is enabled and set up in the full site, users do accrue points when using the Salesforce app. Users can view their points in the full site only though.
- Search is scoped to the community and returns only items from the current community. The only exception is records, since they are shared across communities and the internal organization.
- Role-based external users can approve and reject approval requests from the Approval History related list on records, but they can't submit requests for approval.
- A user's list of notifications includes notifications from all communities the user is a member of. The name of the community in which the notification originated appears after the time stamp.
- External users accessing communities don't see a help link.
- In the Salesforce mobile web, external users' photos don't include any visual indication that the user is an external user. In the full Salesforce site and the Salesforce for Android and Salesforce for iOS, the upper left corner of an external user's photo is orange.
- In the Salesforce mobile web, the People list shows the default photo (☺) next to each user's name. Tap a user to go to their profile page where you can see their uploaded photo. In the Salesforce for Android and Salesforce for iOS, photos appear next to users' names in the People list.
- The community template and your user licenses determine how you can access communities. For more information, see *Access Communities in the Salesforce App* in the Salesforce Help.
- Group members in communities can't edit their email and in-app notification settings in the Salesforce app. As a workaround, users can set their group email notification preference to **Every Post** in the community from the full site. Selecting this option automatically enables both email notifications and in-app notifications for that group.

- Communities aren't available when the mobile device is offline.

SEE ALSO:

Access Communities in the Salesforce App

Navigation and Actions: What's Different or Not Available in the Salesforce App

Navigation

- On most mobile devices, Salesforce is supported in portrait orientation only. The one exception is when using Salesforce for Android and Salesforce for iOS on iPad tablets, where both portrait and landscape orientation are supported.

  The mobile web interface does rotate into landscape orientation but isn't guaranteed to work in this orientation.

- The App Launcher isn't available. You can't switch between standard or custom apps in Salesforce. The navigation menu gives you access to all of the objects and apps that are available to you in the mobile app.
- The Lightning Experience utility bar isn't available.
- The top-down tab-key order, which allows users viewing a record detail page to move through a column of fields from top to bottom before moving focus to the top of the next column of fields, isn't supported. Even if a page layout is configured for a top-down tab-key order, Salesforce moves from left-to-right through field columns.

Actions

- Most actions, including quick actions, productivity actions, and standard and custom buttons, are displayed in the action bar or list item actions.
- The **Save & New** button isn't available.
- If you use URL custom buttons to pass parameters to standard pages in Salesforce Classic—such as pre-populating fields when creating a record—this behavior doesn't work.
- There are a few differences between the Send Email quick action in Salesforce and the standard Email action in Case Feed:
  - Users can't switch between the rich text editor and the plain text editor in a Send Email action.
  - Templates aren't supported in the Send Email action.
  - Quick Text isn't available in the Send Email action.
  - The Send Email action doesn't support attachments.
  - Users can't save messages as drafts when using the Send Email action.
  - Users can't edit or view the From field in the Send Email action.

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

Search Behavior

- Salesforce objects are available when the Smart Search Items option is included in the navigation menu. Smart Search Items is required to get search results for standard and custom objects.
- When doing a global search, you can find records for the objects that appear only in the Recent section of the navigation menu only.

  For the Salesforce for iOS, if you're new to Salesforce and don't yet have a history of recent objects, you can search these objects: Accounts, Cases, Contacts, Files, Leads, Opportunities. You can also search Groups and People if they appear in your Recent section. If they appear in other areas of the navigation menu, they aren't searchable. For Salesforce for Android and mobile web, the default set of objects match the Lightning Experience Navigation Bar that the admin has configured for the Lightning App.

If the user doesn't have access or permissions to the Lightning App, the default set includes Account, Contact, Opportunity, Case, Lead, People (User), and Group objects until the user's most frequently used objects are determined.

As you spend time working in the Salesforce app and the full Salesforce site (Salesforce Classic and Lightning Experience), the objects that you use the most eventually replace the default ones in the Recent section and become the objects that are available for global searches.

- In the Salesforce mobile web, use the search scope bar beneath the global search box to see results for the selected object.

  The objects available in the search scope bar are the same as the items that appear in the Recent section of the navigation menu. The search scope bar displays objects in the same order as in the navigation menu.

  The Salesforce for Android and Salesforce for iOS for Android and iOS don't have a search scope bar. These apps display search results on a single page, grouped by object.

- To find records for an object that doesn't appear in global search results (that is, any of the objects you see when you tap **More** to expand the Recent section in the navigation menu), use the search box on the object's home page.
- You can't pin frequently used items.
- You can't search by divisions.

Instant Results

Note: Instant results are shown as a dropdown menu in the search box and include recent items or auto-suggested records, which are shown after you type at least three characters. If you don't see a record in instant results, perform a full search.

- The Salesforce mobile web shows more recent items and auto-suggested records than in Lightning Experience.
- In the Salesforce mobile web, instant results are displayed for the selected object only, not for multiple objects.

Search Results

- Top Results, which lists search results for the objects you use most frequently, isn't available.
- External Results, which lists search results for the objects from Federated Search, isn't available. However, custom objects created for the purposes of federated search can be added to navigation per the usual process. If used frequently, the object also appears under the Recent section.
- List views aren't included in full search results. To find list views in instant results, open the record search page for an object and type your search terms. As you type, the list of matching items expands to show the list views you've most recently accessed in the full Salesforce site.
- You can't filter search results.
- In the Salesforce for Android and Salesforce for iOS for Android and iOS, global search returns up to 50 of the most relevant records. There's no limit in the Salesforce mobile web.

Lookup Searches

- Instant results are based on recent items only, instead of all records that match the search term.
- A wildcard is appended to all lookup searches.
- Lookup search returns up to 25 of the most relevant records in the results.
- To add records for multiple types of objects within a single lookup, use the dropdown list above the search results.
- Lookup search results don't include Customer Portal or Partner Portal users. However, if the user record was recently viewed, the record appears in lookup instant result suggestions.

Entering Data: What's Different or Not Available in the Salesforce App

There are some differences between the full Salesforce site and the Salesforce app when you're adding new records or updating existing data.

Category	Issue	Creating Records	Editing Records
Any Record	Third-party keyboards aren't supported.	✓	✓
	Inline editing isn't available.	✓	✓
	Changing a record's owner is available for accounts, campaigns, cases, contacts, leads, opportunities, work orders, and custom objects only.		✓
	Combo boxes, which combine a picklist with a text field, aren't available. Typically the text field is available but the picklist is not.	✓	✓
	If territory management is enabled, you can't assign or modify a record's territory rules.	✓	✓
Accounts and Contacts	The **Copy Billing Address to Shipping Address** and **Copy Mailing Address to Other Address** links aren't available.	✓	✓
	If territory management is enabled, the **Evaluate this account against territory rules on save** option isn't available when editing account records.		✓
Events	If two or more contacts are related to an event, the owner can't edit them; if the event has just one related lead or contact, the owner can edit it but not add more.		✓
	Events that aren't related to a contact or object aren't displayed.	✓	✓
	You can't accept or decline an event you've been invited to.		✓
	You can't use Shared Activities to relate multiple contacts to an event.	✓	✓
	The `Related To` field remains editable when the `Name` field is set to *`Lead`*, but you'll receive an error if the `Related To` field contains data when you save the record.	✓	✓
	You can't create recurring events or change the details of a recurring event series. (You can change the details of individual occurrences in an event series.)	✓	✓
	The Subject field doesn't include a picklist of previously defined subjects.	✓	✓
	The Email and Phone fields for an associated contact aren't displayed.	✓	✓
	You can't add attachments.	✓	✓
	You can't send notification emails.	✓	✓
	You can't set event reminders.	✓	✓
Leads	When you add a new lead, the `Campaign` field and the `Assign using active assignment rule" checkbox` aren't available. You can add values to these fields in the full site.	✓	
Opportunities	You can't edit the `Forecast Category` field. The field is automatically populated, based on the value of the `Stage Opportunities` field, when you save the record. You can manually edit the value of this field in Salesforce Classic (but not from Lightning Experience).	✓	✓
Tasks	The `Subject` field doesn't include a picklist of previously defined subjects.	✓	✓

Category	Issue	Creating Records	Editing Records
	The `Related To` field remains editable when the `Name` field is set to *`Lead`*, but you'll receive an error if the `Related To` field contains data when you save the record.	✓	✓
	The `Email` and `Phone` fields for an associated contact aren't displayed.	✓	✓
	You can't use Shared Activities to relate multiple contacts to a task.	✓	✓
	You can't create recurring tasks using a **New Task** quick action, but you can via the **New Task** button on task lists. You can't edit the recurrence details of a recurring task series.	✓	✓
	You can't add attachments.	✓	✓
	You can't send notification emails.	✓	✓
	You can't set task reminders.	✓	✓
Phone Number Fields	The keypad that displays in phone number fields doesn't include parentheses, hyphens, or periods, and doesn't apply any phone number formatting when you save the record. To apply a specific phone number format, edit the record in the full site.	✓	✓
Success Message	After creating a record from a related list in the Salesforce app, the resulting success message doesn't include a link to the new record (like in Lightning Experience).	✓	

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

Approval Responses

You can't unlock a record that's locked for approval.

Salesforce App Notifications for Approval Requests

- Notifications for approval requests aren't sent to queues or delegates. For each approval step involving a queue, add individual users as assigned approvers, so at least those individuals can receive the approval request notifications in the mobile app. To have both queues and individual users as assigned approvers, select **Automatically assign to approver(s)** instead of **Automatically assign to queue** in the approval step.
- Notifications for approval requests are sent only to users who have access to the record being approved. Assigned approvers who don't have record access can still receive email approval notifications, but they can't complete the approval request until someone grants record access.

Approvals in Chatter

In the Salesforce app, you can't respond to approval requests from Chatter. To respond to approval requests, go to the Approvals navigation item.

Approval Comments

- The Salesforce app prompts you for comments after you tap Approve or Reject.
- The Approval History related list displays truncated comments. To see the full comment for a given approval instance, tap the instance, then tap **Comments**.

Approval History Related List

- The Approval History related list doesn't include the Submit for Approval button.

- When working with approvals in communities, role-based external users can see and take action from the Approval History related list, but they can't submit requests for approval.

Offline Access: What's Different or Not Available in the Salesforce App

Access Data While Offline

When caching is enabled, Salesforce for Android and Salesforce for iOS users can access cached data while working offline. The default data that's cached includes recently accessed records for the first five objects in the Recent section of the user's navigation menu, plus the user's recent tasks and dashboards. Recently accessed records are determined by a user's activities in both the Salesforce app and the full Salesforce site, including Salesforce Classic and Lightning Experience. In addition, much of the data that a user accesses throughout a Salesforce session is added to the cache.

Some data isn't available when a user's mobile device is offline. See Data and UI Elements That Are Available When the Salesforce App is Offline for the full rundown on what's supported.

Update Data While Offline (Beta)

Create, Edit, and Delete Actions

- Create records using the **New** button on recently accessed object home pages. New record actions in an action bar (such as **New Task**, **New Contact**, or **New** on related lists) aren't supported offline.
- **Edit** and **Delete** actions in the action bar are available for cached records only.

All Other Quick Actions

- All other action bar icons, such as **Log a Call**, **Post**, or **Change Owner**, aren't supported offline.

Record Types for Recent Objects

- Salesforce caches up to 15 of a user's most recently accessed record types per object. If your org has defined more than 15 record types for any of a user's recent objects (that is, the first five objects listed in the Recent section of the user's navigation menu), only the cached record types are available when creating a record offline. And only records matching the cached record types are editable while offline.

Lookups and Picklists

- Dependent lookups and picklists for a cached record aren't supported when offline, unless the user interacted with these elements before the record was cached.
- Lookup filters aren't supported when offline. Users can enter the name of the related lookup record when editing data offline but the app doesn't search for related looked records until the user's mobile device is back online.
- Complex page layouts, with a very large number of fields or many picklists, can result in records that are too large to cache. If a user doesn't see expected recently accessed records when offline, this may be the reason why. If this becomes a problem for your users, we recommend re-evaluating the affected object's page layout to see if you can optimize it for mobile use.

Notes

- Notes that include images aren't available offline.
- Images can't be added to notes when working offline.
- Users can't relate notes to records when working offline.

Events

- If you create an event when working offline, it is in draft mode until Salesforce is back online. However, there is no visual cue on the Events list that the event is still in draft mode.

Tasks

- Users can only create tasks offline if the simplified New Task form on mobile is disabled.
  1. From Setup, enter `Activity Settings` in the `Quick Find` box, then select **Activity Settings**.
  2. Deselect **Show simpler New Task form on mobile**.
  3. Click **Submit**.
- Selecting or deselecting checkboxes on tasks isn't supported when offline.

Communities

- Salesforce Communities aren't supported when offline.

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

Custom Home Pages

- The Salesforce app doesn't support login redirection to other Salesforce apps or custom home tabs like the full Salesforce site does. If you prefer to retain this redirection for users who log in to Salesforce mobile web, turn off Salesforce mobile web. This can be done on a user-by-user basis or for your entire organization.

Custom Actions and Buttons

- Custom buttons that are added to the Button section of a page layout and that define the content source as *`URL`* or *`Visualforce`* are supported in the Salesforce app. Remember that Visualforce pages must be enabled for use in the Salesforce app.

  Custom links, custom buttons that are added to list views, and custom buttons that define the content source as *`OnClick JavaScript`* aren't available in the Salesforce app.
- Using URL custom buttons to pass parameters to standard pages in Salesforce Classic—such as pre-populating fields when creating a record—doesn't work in the Salesforce app or Lightning Experience.
- Custom images used for action icons must be less than 1 MB in size.

Lightning Pages

- You can't add more than 25 components to a Lightning page region.

Visualforce Pages

- Standard tabs, custom object tabs, and list views that are overridden with a Visualforce page aren't supported. The Visualforce page is shown for full site users but app users will see the default Salesforce page for the object instead. This restriction exists to maintain the app experience for objects.
- The Salesforce app imposes additional resrictions and constraints on Visualforce pages. See Visualforce Guidelines and Best Practices in the Salesforce App Developer guide for details.

Programmatic Customizations

- These programmatic customizations to the UI aren't supported: Web tabs and S-controls.

Help Users From Anywhere With SalesforceA

SalesforceA is a mobile app for Salesforce administrators. When you're away from your desk, you can use your phone or tablet to perform essential administration tasks like resetting passwords, freezing users, and viewing current system status.

SalesforceA is free. Download it from the Google Play Store for Android phones and tablets, and from the Apple App Store for Apple iPhone, iPod Touch, and iPad.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To use SalesforceA:

- Manage Users

IN THIS SECTION:

SalesforceA Options

Manage users and view information for Salesforce organizations from your mobile device.

Log In to SalesforceA

Log in to the SalesforceA mobile app to perform essential administrative tasks for your Salesforce organization.

Log In to Multiple Organizations with SalesforceA

Use SalesforceA on your mobile device to log in to multiple Salesforce organizations that you administer. Once logged in, you can switch between organizations without going through the login process again.

Create a New User with SalesforceA

Use SalesforceA on your mobile device to create a new user. Creating a new user is available in SalesforceA for iOS version 3.3 or later.

Reassign a User License with SalesforceA

When you create a new user with SalesforceA, there may be instances when your org doesn't have enough user licenses to assign to the newly created user. No need to worry if this happens, because SalesforceA saves the newly created user as inactive. To change the newly created user from inactive to active, you can reassign a user license from an existing user to the newly created user. Reassigning a user license is available in SalesforceA for iOS version 3.3 or later.

SalesforceA Options

Manage users and view information for Salesforce organizations from your mobile device.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

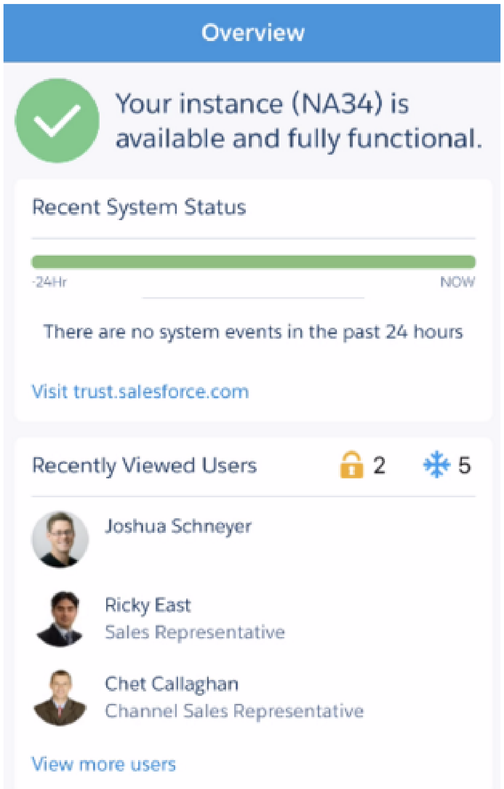
To use SalesforceA:

- Manage Users

Overview of Your Organization

The Overview screen shows:

- Number of frozen and locked out users
- Trust status
- Recently viewed users



Overview

Your instance (NA34) is available and fully functional.

Recent System Status

-24Hr NOW

There are no system events in the past 24 hours

Visit trust.salesforce.com

Recently Viewed Users 🔓 2 ❄ 5

Joshua Schneyer

Ricky East
Sales Representative

Chet Callaghan
Channel Sales Representative

View more users

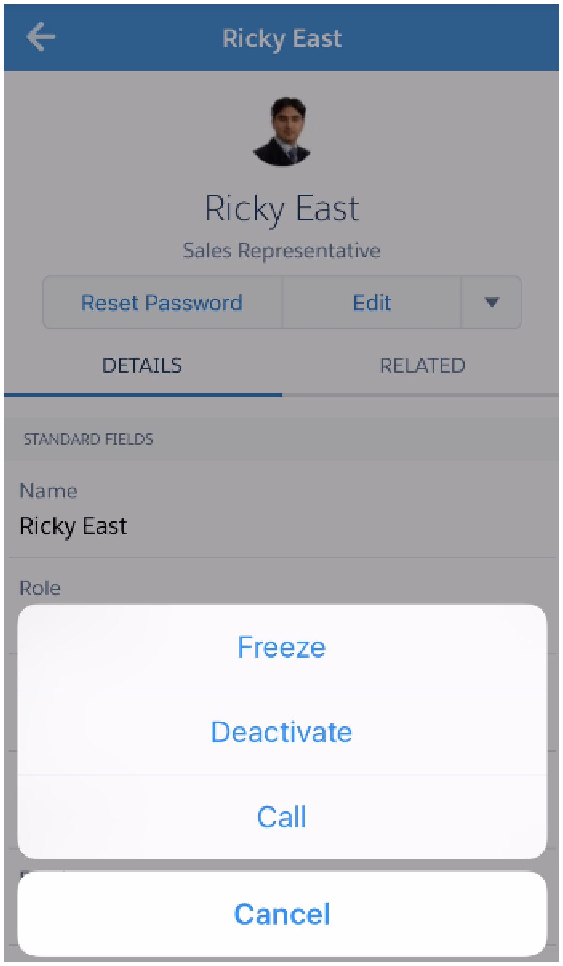
For Android users, the navigation icon is in the top left. Tap it to go to the navigation menu.

For iOS users, navigation is done through the action bar at the bottom of the screen.

User Management

From the navigation menu, tap **Users** to see a list of users or search for a user. Tap a name to:

- View or edit user details
- Freeze, deactivate, or reactivate the user
- Reset a user password
- Assign permission sets (iOS only)
- Create a new user (iOS only)



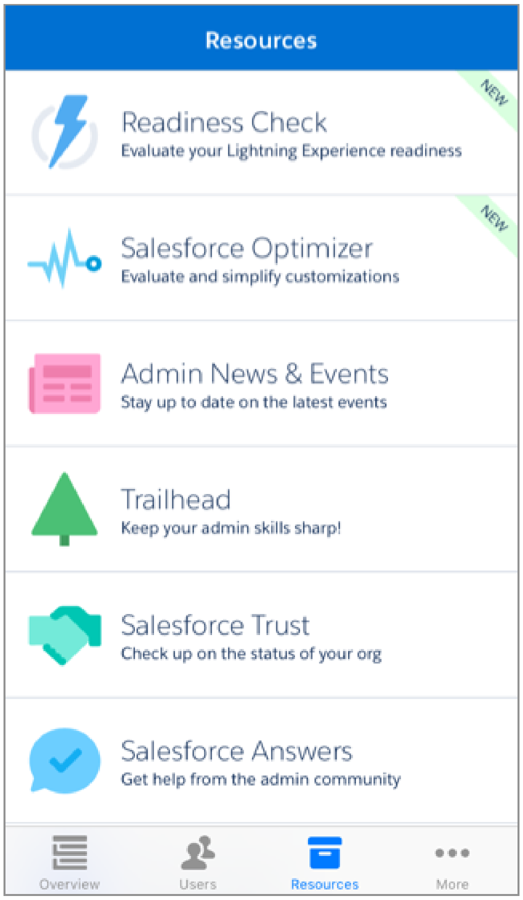
Swipe to the Related page to see:

- The user's current permission sets
- The user's login history

Additional Information

The Resources page gives you quick access to:

- Lightning Readiness Check
- Optimizer
- Admin News and Events
- Trailhead
- Salesforce Trust
- Salesforce Answers
- Salesforce Release Notes



Resources

Readiness Check
Evaluate your Lightning Experience readiness

Salesforce Optimizer
Evaluate and simplify customizations

Admin News & Events
Stay up to date on the latest events

Trailhead
Keep your admin skills sharp!

Salesforce Trust
Check up on the status of your org

Salesforce Answers
Get help from the admin community

Log In to SalesforceA

Log in to the SalesforceA mobile app to perform essential administrative tasks for your Salesforce organization.

As a Salesforce administrator, you can use SalesforceA to log in to your production organization (default), sandbox environment, or a custom host. Choose the environment or host with the host menu.

- For iOS users: open the host menu from the gear icon in the upper right corner of the login screen.
- For Android users: open the host menu from the action overflow button in the upper right corner of the login screen.

If prompted, enter a passcode as an extra layer of security for your mobile device. Manage this security setting in the Salesforce desktop browser application from **Setup** in the **Connected Apps** entry for **SalesforceA**.

Once you log in, you see the Overview screen.

EDITIONS

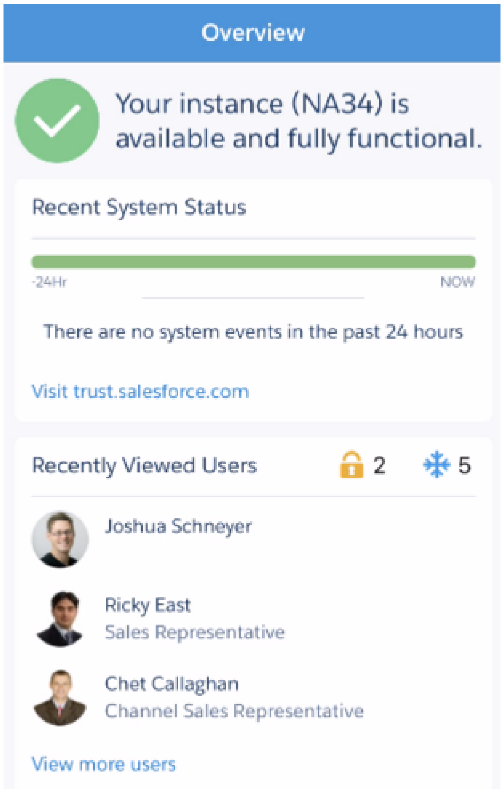
Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To use SalesforceA:

- Manage Users



Overview

Your instance (NA34) is available and fully functional.

Recent System Status

-24Hr NOW

There are no system events in the past 24 hours

Visit trust.salesforce.com

Recently Viewed Users 🔒 2 ❄ 5

Joshua Schneyer

Ricky East
Sales Representative

Chet Callaghan
Channel Sales Representative

View more users

SEE ALSO:

Log In to Multiple Organizations with SalesforceA

Log In to Multiple Organizations with SalesforceA

Use SalesforceA on your mobile device to log in to multiple Salesforce organizations that you administer. Once logged in, you can switch between organizations without going through the login process again.

1. Tap the navigation icon to go to the menu. For iOS users, tap **More**.
2. Tap the down arrow next to your username. A list of your accounts appears.
3. Select a previously saved username or tap **+ Add account** to add an account.
4. To choose a sandbox or custom host, tap the gear icon in the upper right (iOS users) or the action overflow button in the upper right (Android users), and switch to your desired host.

From the list of your accounts, you can:

- Switch between organizations
- See whether each organization is production or sandbox (iOS only)
- See each organization’s edition (iOS only)

Tap the up arrow to close the account selector.

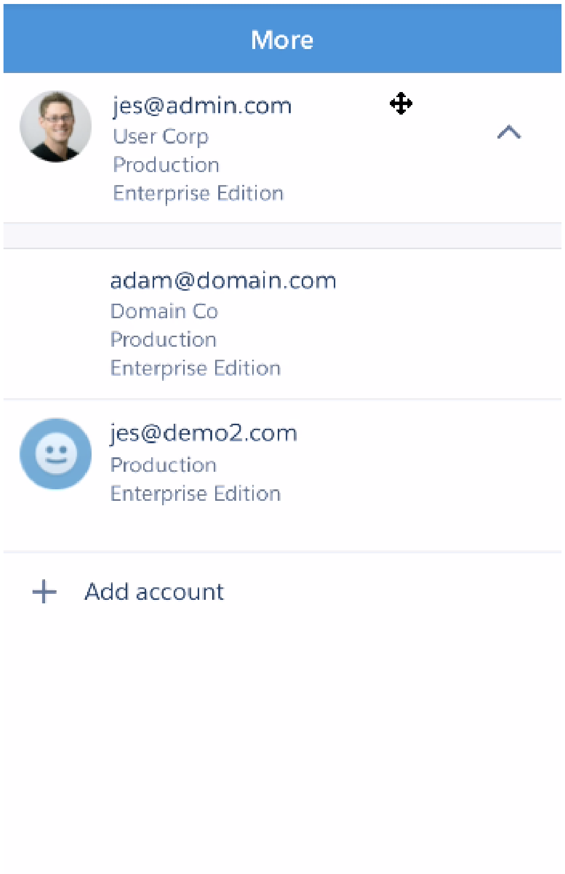
EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To use SalesforceA:
- Manage Users



Create a New User with SalesforceA

Use SalesforceA on your mobile device to create a new user. Creating a new user is available in SalesforceA for iOS version 3.3 or later.

1. From the **Users** page, tap **+**.
2. Enter the user's name and email address and a unique username in the form of an email address. By default, the username is the same as the email address.
3. Select a `User License`. The user license determines which profiles are available for the user.
4. Select a profile, which specifies the user's minimum permissions and access settings.
5. In Professional, Enterprise, Unlimited, Performance, and Developer Editions, select a `Role`.
6. Select `Generate new password and notify user immediately` to have the user's login name and a temporary password emailed to the new user.
7. Tap **Save**.

Note: Your *username* must be unique across all Salesforce orgs. The username must be in the format of an email address, for example, jane@salesforce.com. This email username doesn't have to work. You *can* have the same functioning email address associated with your account across orgs—only the *username in the form of an email address* must remain unique.

EDITIONS

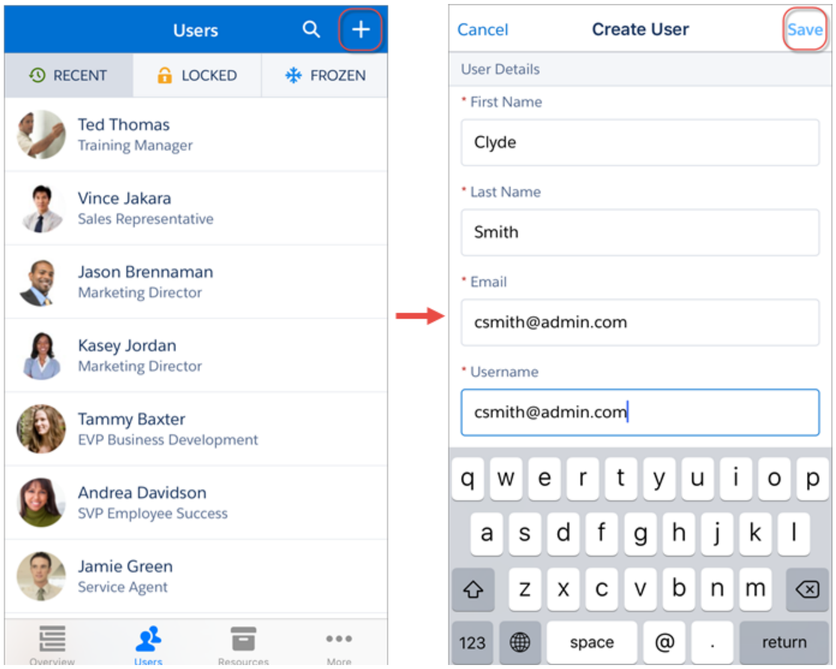
Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To use SalesforceA:

- Manage Users



Ted Thomas
Training Manager

Vince Jakara
Sales Representative

Jason Brennaman
Marketing Director

Kasey Jordan
Marketing Director

Tammy Baxter
EVP Business Development

Andrea Davidson
SVP Employee Success

Jamie Green
Service Agent

User Details

* First Name: Clyde

* Last Name: Smith

* Email: csmith@admin.com

* Username: csmith@admin.com

You can create a new user even if you don't have enough user licenses to accommodate one. SalesforceA saves all the fields of your new user, but the user is in an inactive state. To change the state of an inactive user to active, you need to reassign a license from an existing user to your newly created user. For guidelines about creating a new user, see Guidelines for Adding Users in the Salesforce Help for more information.

Reassign a User License with SalesforceA

When you create a new user with SalesforceA, there may be instances when your org doesn't have enough user licenses to assign to the newly created user. No need to worry if this happens, because SalesforceA saves the newly created user as inactive. To change the newly created user from inactive to active, you can reassign a user license from an existing user to the newly created user. Reassigning a user license is available in SalesforceA for iOS version 3.3 or later.

1. From the inactive user's page, tap **Reassign a License**.
2. Either scroll or use the **Find User** search bar to find an existing user you want to reassign a user license from.
3. When you've found that existing user, tap **Reassign This License**.
4. Confirm the changes, and tap **OK**.

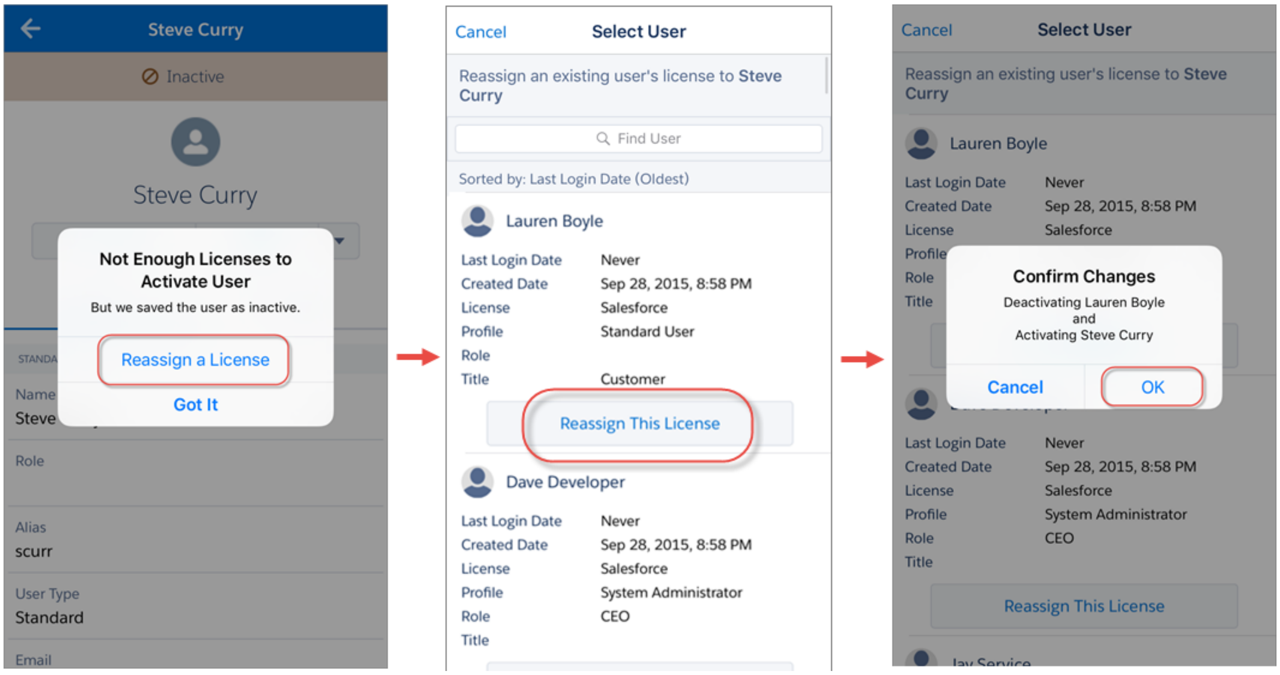
EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To use SalesforceA:
- Manage Users



Not Enough Licenses to Activate User

But we saved the user as inactive.

Name
Steve

Role

Alias
scurr

User Type
Standard

Email

Reassign an existing user's license to Steve Curry

Sorted by: Last Login Date (Oldest)

Lauren Boyle

Last Login Date	Never
Created Date	Sep 28, 2015, 8:58 PM
License	Salesforce
Profile	Standard User
Role	
Title	Customer

Dave Developer

Last Login Date	Never
Created Date	Sep 28, 2015, 8:58 PM
License	Salesforce
Profile	System Administrator
Role	CEO
Title	

Confirm Changes

Deactivating Lauren Boyle
and
Activating Steve Curry

Salesforce Chatter

Salesforce Chatter is a downloadable app for Windows 10 Anniversary Edition users. Salesforce Chatter combines Chatter feeds and posting functionality with the power of an app optimized for Windows 10 users.

Using the Salesforce Chatter app, you only have to log in to Salesforce once to access everything Salesforce has to offer in the app and the full site. You can launch directly into the full Salesforce site to view Lightning Experience pages, saving time and getting to information you need most faster. On the Windows Surface Pro 4, you can attach drawings made in the app to Chatter posts for new ways of collaborating on projects and sharing updates.

IN THIS SECTION:

Requirements for the Salesforce Chatter App

Salesforce Chatter is supported for devices running Windows Anniversary Edition.

Salesforce performs automated and manual testing of devices running the Windows 10 Anniversary Edition only.

Customers aren’t blocked from using Salesforce Chatter on untested operating systems. The operating systems are subject to change, with or without notice.

Get the Salesforce Chatter App

Salesforce Chatter is available from the Windows Store. Devices must be running Windows 10 Anniversary Edition.

Install Salesforce Chatter

The Salesforce Chatter downloadable app is available for Windows 10 Anniversary Edition users. You can download and install Salesforce Chatter from the Windows Store.

Once the app is installed, launch it from your home screen and log in to your Salesforce account.

Note: If you're not able to log in, verify with your Salesforce admin that you're enabled to use the downloadable app.

What's Available in the Salesforce Chatter App

Salesforce Chatter gives you more ways than ever to collaborate with coworkers using Chatter. Salesforce Chatter requires only a single authentication to access all of Salesforce. You can also attach drawings directly from the app to Chatter posts.

IN THIS SECTION:

Post Drawings with Salesforce Chatter

You can post drawings made with the Salesforce Chatter canvas directly on to Chatter posts on touch enabled Windows 10 devices.

Create a new Chatter post and tap **Draw** to launch the canvas.

Once inside the canvas, use the ruler feature for straight lines, or draw with a stylus or finger. Once your drawing is complete tap **Attach**.

You can share more context for your drawing in the Chatter post, or tag coworkers and groups to share the drawing with them specifically.

Tap **Post** to share the drawing in your Chatter feed or with a group depending on the audience of your post.

Authenticate Once with Salesforce Chatter

Salesforce Chatter makes getting to work in the full Salesforce site easier than ever. Just log in to the Salesforce Chatter app and launch the full Salesforce site directly from the app.

Tap **Full Site** in the left navigation menu to launch your Salesforce homepage. You can also open a specific Chatter post, file, or image in Lightning Experience directly in your browser by tapping ⌄ and **Open in browser**.

Support On-the-Go Productivity with Salesforce Mobile Classic

Salesforce Mobile Classic helps your teams succeed by allowing users to access their latest Salesforce data, whenever and wherever they need it, directly from Android™ and iPhone® devices.

The Salesforce Mobile Classic app exchanges data with Salesforce over mobile or wireless networks, and stores a local copy of the user's data in its own database on the mobile device. Users can edit local copies of their Salesforce records when a data connection isn't available, and transmit those changes to Salesforce when a connection is available again. The app also promotes near real-time logging of critical information by prompting users to enter updates directly in Salesforce or Force.com AppExchange apps after important customer calls, emails, or appointments.

A Salesforce Mobile Classic license is required for each user to use Salesforce Mobile Classic. For organizations using Unlimited, Performance, and Developer Editions, Salesforce provides one mobile license for each Salesforce license. Organizations using Professional or Enterprise Editions purchased mobile licenses separately.

Note: The Android and iPhone apps are available in English, Japanese, French, German, and Spanish. Contact Salesforce to turn on Salesforce Mobile Classic for your organization.

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

IN THIS SECTION:

About the Salesforce Mobile Classic Default Configuration

Salesforce Mobile Classic Implementation Tips and Best Practices

Set up the Salesforce Mobile Classic app using these tips and best practices.

Setting Up Salesforce Mobile Classic

Manage Salesforce Mobile Classic Configurations

Manage Salesforce Mobile Classic Devices

Customize Salesforce Mobile Classic Settings

Salesforce Mobile Classic App Limits

SEE ALSO:

Setting Up Salesforce Mobile Classic

Salesforce Classic Implementation Guide

Salesforce Classic User Guide for iPhone

About the Salesforce Mobile Classic Default Configuration

Mobile configurations for the Salesforce Mobile Classic app are sets of parameters that determine what data Salesforce transmits to users' mobile devices and which users receive the data on their mobile devices. A default mobile configuration is provided for Professional, Enterprise, Unlimited, Performance, and Developer Edition organizations. Administrators can't view or edit the default mobile configuration.

Users are automatically assigned to the default mobile configuration when they activate their Salesforce account from a supported mobile device using the Salesforce Mobile Classic app.

The default mobile configuration:

- Allows users with an assigned mobile license to install and activate Salesforce Mobile Classic, even if you haven't yet assigned them to a mobile configuration.

You can disable Salesforce Mobile Classic to prevent users from activating the Salesforce Mobile Classic app.

The default configuration can mobilize the following objects:

- Accounts
- Assets
- Cases
- Contacts
- Dashboards
- Events
- Leads
- Opportunities
- Reports
- Solutions
- Tasks

Note:

- Not all objects available in the Salesforce Mobile Classic app are mobilized with the default configuration.
- Assets aren't available as a tab in the Salesforce Mobile Classic app but display as a related list for accounts, cases, and contacts.
- Accounts include both business and person accounts. To exclude person accounts from the configuration's data set, use the "`Is Person Account equals False`. criteria" To use only person accounts, use "`Is Person Account equals True`." If a mobile configuration includes accounts but not contacts, users assigned to that configuration see a Contacts tab in the mobile client application, and the tab contains person accounts.

The default configuration automatically synchronizes records the user recently accessed in Salesforce on the Salesforce Mobile Classic app. Users can search for records that aren't automatically synchronized; once the user downloads a record, the record becomes a permanent part of the data set. In addition to recently accessed records, the default configuration synchronizes activities closed in the past five days and open activities due in the next 30 days.

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

Salesforce Mobile Classic Implementation Tips and Best Practices

Set up the Salesforce Mobile Classic app using these tips and best practices.

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic configurations:

- View Setup and Configuration

To create, change, or delete Salesforce Mobile Classic configurations:

- Manage Mobile Configurations

Building Lean Data Sets

- Keep the data sets in your mobile configurations as small as possible. Not only do lean data sets greatly improve the Salesforce Mobile Classic app's performance, but they also make the app easier to use. Pushing massive amounts of data to the device might seem like a good idea, but the important records tend to get lost among the ones that aren't relevant to users' day-to-day activities. Small data sets are powerful because the Salesforce Mobile Classic app synchronizes with Salesforce every 20 minutes, so the data is constantly refreshed with new and updated records. Even if your mobile configurations don't account for every possible record your users might need, they can search for records that aren't automatically synchronized to their devices.

  To build small data sets:

  - Nest the objects in the data set tree. For example, add contacts as a child data set of the account object so that the data set includes contacts related to the mobilized accounts instead of all the user's contacts.
  - Avoid setting the record ownership filter to All Records unless your organization uses a private sharing model. It's unlikely that users need to see all of an object's records on their devices. Instead of mobilizing all opportunity records, for example, mobilize just the opportunities owned by the user or the user's opportunity team.
  - Use filters that synchronize the most relevant records. For example, even if you limit the opportunities on the device to records owned by the user, you could further prune the data set by mobilizing only opportunities closing this month.
  - Set a record limit to prevent the data set from getting too large. Generally, a single data set should generate no more than 2,500 records.
- Another way to build lean data sets is to mobilize the Salesforce recent items list, add the data sets, and set the record ownership filters in your data sets to None (Search Only). The user's data set is populated with records recently accessed in Salesforce, and those records in turn synchronize additional data based on the data set hierarchy. For example, let's say you create a data set with the account object at the root level and add the contact, task, and event objects as child data sets. When the Salesforce Mobile Classic app synchronizes an account from the Salesforce recent items list, it also synchronizes the contacts, tasks, and events related to that account.
- If you're not sure which fields to use as filters for your data sets or mobile views, consider using the Last Activity Date field. For example, set up a filter that synchronizes contacts with an activity logged this week or this month. The Last Activity Date field is a better indicator of a record's relevance than the Last Modified Date field—often the main detail of a record remains unchanged even though users frequently log related tasks and events.

Mobilizing Records Users Need

- Before mobilizing a custom object, make sure the object's functionality is compatible with the Salesforce Mobile Classic app. Salesforce Mobile Classic doesn't support S-controls, mashups, merge fields, image fields, or custom links.
- To obtain a relevant set of activities, mobilize the task and event objects at the root level of the data set hierarchy and nest them under parent objects, like contacts, accounts, and opportunities. Adding tasks and events at multiple levels ensures that users will see their personal activities and activities related to the records on their devices. Avoid mobilizing too much activity history or too

many tasks and events not owned by the user. Generally, there are more task and event records in an organization than any other type of record, so it's easy to bloat data sets with too many activities.

- If your sales representatives frequently take orders in the field and need a comprehensive inventory list, add the product object at the root level of the data set hierarchy. Nesting the opportunity product object below the opportunity object won't mobilize all products.
- If your users need to assign tasks to other users or change the record owner, mobilize the user object so that the names of other users will be available on the device. Avoid mobilizing all user records—instead, set up filters based on the role or profile.
- Be sure that users assigned to a mobile configuration have field-level access to all the fields used in the configuration's filter criteria. If a user doesn't have access to a field in a data set's filter criteria, the Salesforce Mobile Classic app won't synchronize the records for that data set or its child data sets.
- You can sometimes use cross-object formula fields to work around limitations of the Salesforce Mobile Classic app. For example, Salesforce Mobile Classic doesn't support campaigns, so you can't add the campaign object as a data set and add the opportunity object as its child data set to get the related records. However, you can create a text formula field on the opportunity object equal to the name of the parent campaign. The field needs to be visible, but it doesn't need to be included on your page layouts. Then add the opportunity object to the data set and use the new formula field to filter opportunities related to a specific campaign.
- Although a mobile configuration might include an object at multiple levels in the data set hierarchy, users won't see duplicate tabs in the Salesforce Mobile Classic app. Only one Task tab appears on the device even if you mobilize the task object at the root level and as a child data set of three objects.

Customizing Mobile Configurations

- Clean up your mobile page layouts by excluding fields from the objects in the mobile configuration. Less data is sent to the device, and mobile users don't have to scroll through unnecessary fields.
- If you mobilize the Dashboards tab, be sure to select any other tabs that should appear in the Salesforce Mobile Classic app. Customizing the tabs for a mobile configuration overrides the default tab set—if you only mobilize the Dashboard tab, it will be the only tab sent to the device.
- Due to the small size of mobile device screens, you can only select two display columns for mobile views. If you need three columns of data, create a text formula field on the object that concatenates the three fields, then use the formula field in the mobile view criteria.
- When creating mobile views, you can filter based on the current user with the $User.ID global variable, but you can't enter a user's name as a value in the filter criteria. To build a view based on users, create a text formula field on the appropriate object, then use the formula field in the mobile view criteria. For example, to create a view that displays opportunities owned by an opportunity team, create a text formula field on the opportunity object that contains the opportunity owner's user ID or role, then create a view that filters on values in that field.

Testing and Deploying the Mobile Product

- It's important to test mobile configurations to make sure they're synchronizing an acceptable amount of data. Test configurations against active users who own a very large number of records. Typically, most data sets generate between 500 KB and 4 MB of data. If the data sets are over 4 MB, refine the filter criteria to limit the amount of data sent to the device.
- You can use the Salesforce Mobile Classic app in the sandbox before deploying to your organization.
- Use of the Salesforce Mobile Classic app requires a data plan. The wireless data volume for the Salesforce Mobile Classic app varies greatly between customers and even users in the same organization. It's impossible to predict your organization's data usage, but we can offer some guidelines:
  - The initial data download consists of records that match the criteria specified in the user's mobile configuration and the metadata needed to support these records when disconnected. On average, the data sizes range from 500 KB–4 MB.

  - After the initial download of data, incremental update requests are initiated by the client app every 20 minutes. Each of these requests and the corresponding server response are approximately 200 bytes.
  - If any new data is downloaded to the client app as a result of the update request, only the new or changed values are sent. For example, the Salesforce Mobile Classic app only downloads the new phone number in a contact record, not the entire contact record. The amount of data transmitted differs for every organization and every user.

Generally, the volume of data transmitted by the Salesforce Mobile Classic app is low compared to moderate email usage.

Best Practices

- Use the zero-administration deployment option to experiment with the Salesforce Mobile Classic app before you set up mobile configurations. You'll create better blueprints for your mobile configurations if you've tried using the Salesforce Mobile Classic app.
- Talk to users about their favorite reports, views, and dashboards to get ideas for what filter criteria to use in mobile configurations.
- After setting up mobile configurations, deploy the Salesforce Mobile Classic app on a limited basis with a select group of users. Adjust the mobile setup based on their feedback, then deploy to all of your users.

Setting Up Salesforce Mobile Classic

To deploy the Salesforce Mobile Classic app to your organization:

1. Review the mobile implementation tips and best practices
2. Enable mobile users
3. Create one or more mobile configurations
4. Define the data sets for your mobile configurations
5. Test the mobile configurations
6. Customize mobile page layouts and adjust mobile user permissions (optional)
7. Customize mobile tabs (optional)
8. Create custom mobile views (optional)
9. Set up mobile reports (optional)
10. Set up Salesforce CRM Content (optional)
11. Configure access for partner users (optional)
12. Create links to Web and Visualforce Mobile pages (optional)
13. Notify users that Salesforce Mobile Classic is available for download

When users download the Salesforce Mobile Classic app and activate their accounts, you can manage their devices in the Salesforce Mobile Classic Administration Console.

SEE ALSO:

Manage Salesforce Mobile Classic Configurations

Manage Salesforce Mobile Classic Devices

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic settings:

- View Setup and Configuration

To change Salesforce Mobile Classic settings:

- Manage Mobile Configurations

Enabling Salesforce Mobile Classic Users

To enable users to access Salesforce Mobile Classic:

1. Allocate mobile licenses to users by selecting the `Salesforce Mobile Classic User` checkbox on the user record.
2. Edit each custom profile to which Salesforce Mobile Classic users are assigned to include the "API Enabled" permission. Salesforce Mobile Classic users need access to the API so their mobile devices can communicate with Salesforce. The "API Enabled" permission is enabled by default on standard profiles.

Note: The Android and iPhone apps are available in English, Japanese, French, German, and Spanish. Contact Salesforce to turn on Salesforce Mobile Classic for your organization.

To prevent users from activating Salesforce Mobile Classic on their mobile devices before you're ready to deploy the app, disable the `Salesforce Mobile Classic User` checkbox for all your users.

Note: If you deselect this checkbox for a user who is already assigned to a mobile configuration, Salesforce removes that user from the mobile configuration and assigns the user to the default mobile configuration.

The free version of Salesforce Mobile Classic is available only for orgs that enabled this option before Summer '16. With Summer '16, all other orgs (new and existing) don't see this option.

SEE ALSO:

Salesforce Classic Implementation Guide

Salesforce Classic User Guide for iPhone

Setting Up Salesforce Mobile Classic

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic settings:

- View Setup and Configuration

To change Salesforce Mobile Classic settings:

- Manage Mobile Configurations

Create Salesforce Mobile Classic Configurations

Mobile configurations are sets of parameters that determine the data Salesforce transmits to users' mobile devices, and which users receive that data on their mobile devices. Organizations can create multiple mobile configurations to simultaneously suit the needs of different types of mobile users. For example, one mobile configuration might send leads and opportunities to the sales division, while another mobile configuration sends cases to customer support representatives.

Before creating your mobile configurations, plan which profiles and users you want to assign to each configuration. Each mobile configuration only affects the mobile devices of users assigned to the configuration.

To create a mobile configuration:

1. Enter Basic Information
2. Assign Users and Profiles
3. Set Total Data Size Limit
4. Complete Your Mobile Configuration

Note: A default mobile configuration is provided for Professional, Enterprise, Unlimited, Performance, and Developer Edition organizations. You can't view or edit the default configuration.

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic configurations:

- View Setup and Configuration

To create, change, or delete Salesforce Mobile Classic configurations:

- Manage Mobile Configurations

Enter Basic Information

1. From Setup, enter `Salesforce Classic Configurations` in the `Quick Find` box, then select **Salesforce Classic Configurations** to access the mobile configurations list page.
2. Click **New Mobile Configuration**.
3. Enter a name for the mobile configuration.
4. Select the `Active` checkbox if you want to activate the mobile configuration immediately after creating it. The mobile configuration does not work until you select this checkbox.

   If you deactivate an active mobile configuration, Salesforce saves all requests from devices of the users assigned to the mobile configuration for up to one week. If you reactivate the mobile configuration, Salesforce executes those requests in the order received.
5. Optionally, enter a description for the mobile configuration.
6. Optionally, select the `Mobilize Recent Items` checkbox to mark recently used records in Salesforce for device synchronization.

   Selecting this option ensures that mobile users assigned to the configuration will not have to search for and download items they recently accessed on Salesforce, even if those records do not meet the configuration's filter criteria. Only records belonging to mobilized objects can be marked for device synchronization; for example, if you do not mobilize the account object in a configuration, users assigned to that configuration cannot automatically receive recent accounts on their devices.
7. If you select the `Mobilize Recent Items` checkbox, select a value from the `Maximum Number of Recent Items` drop-down list. Set a low number if your users have minimal free space on their mobile devices.
8. Optionally, select the `Mobilize Followed Records` checkbox to automatically synchronize records users are following in Chatter to their mobile device. The device only synchronizes followed records for objects included in the mobile configuration's data set.

   The `Mobilize Followed Records` checkbox is only available if Chatter is enabled for your organization.

Assign Users and Profiles

You can assign individual users and profiles to each mobile configuration. If you assign a profile to a mobile configuration, the mobile configuration applies to all Salesforce Mobile Classic users with that profile unless a specific user is assigned to another mobile configuration.

Tip: For ease of administration, we recommend that you assign mobile configurations to profiles; however, you may have situations in which you need to assign a configuration directly to individual users.

To assign users and profiles to a mobile configuration:

1. In the Search drop-down list, select the type of member to add: users or profiles. This drop-down list is not available if you have not enabled the `Mobile User` checkbox on any user records, or if all users are already assigned to a mobile configuration; in that case, you can only assign profiles to this mobile configuration.
2. If you do not immediately see the member you want to add, enter keywords in the search box and click **Find**.
3. Select users and profiles from the `Available Members` box, and click the **Add** arrow to add them to the mobile configuration.

   You can assign each user and profile to only one mobile configuration.

   The `Available Members` box only displays users who have the `Mobile User` checkbox enabled.
4. If there are users or profiles in the `Assigned Members` box you do not want to assign to this mobile configuration, select those users and click the **Remove** arrow.

   Warning: Removing a user from an active mobile configuration deletes the Salesforce-related data on the user's mobile device but does not delete the client application.

Set Total Data Size Limit

Different types of mobile devices offer different memory capacities, and some devices experience serious problems if all of the flash memory is used. To avoid overloading mobile devices, optionally specify a total data size limit for each mobile configuration. The total data size limit prevents Salesforce from sending too much data to the mobile devices of users assigned to the mobile configuration.

To set the total data size limit, use the `Don't sync if data size exceeds` drop-down list to specify the amount of memory that is consistently available on the mobile devices of users who are assigned to this mobile configuration. If the combined size of all the data sets exceeds this limit, users assigned to this profile receive an error message on their mobile devices, and Salesforce will not synchronize any data sets in this mobile configuration. Test your mobile configuration to make sure the data sets do not exceed the total data size limit.

Tip: To reduce the size of your data, do one or more of the following:

- Delete a data set.
- Reduce the scope of your data sets.
- Refine the filter criteria of your data sets.

Complete Your Mobile Configuration

Click **Save**. Note that your mobile configuration is not active until you select the `Active` checkbox.

SEE ALSO:

Manage Salesforce Mobile Classic Configurations

Define Data Sets

Setting Up Salesforce Mobile Classic

Define Data Sets

Accessing Salesforce from a mobile device is very different than accessing it from your computer. This is because mobile devices generally have less memory and screen size than computers, and they do not maintain a constant network connection. To work with these limitations, each mobile configuration only transfers data sets, which are subsets of the records users access in the Salesforce online user interface. Mobile devices store data sets in on-board databases, allowing users to access their most important records and work offline when no network connection is available. Salesforce automatically synchronizes the on-board databases when the mobile device reestablishes a network connection.

Each data set can contain records related to a single object and is classified by the name of that object. For example, the Accounts data set only includes account records.

Data sets can have child data sets, which are data sets that contain records associated with a top-level (parent) data set. For example, if the first level of your hierarchy has an Accounts data set, you can add a Contacts child data set that includes all contact records related to the account records. Child data sets appear as related lists on mobile devices.

A single mobile configuration can have multiple data sets for the same object and at different levels. For example, you can have an Events parent data set and an Events child data set under Leads.

Tip: Review the sample data sets to see how you might define data sets for common groups of Salesforce users.

After creating a mobile configuration, you must define its data sets. To access the data sets for a mobile configuration:

1. From Setup, enter *Salesforce Classic Configurations* in the `Quick Find` box, then select **Salesforce Classic Configurations**. Then click the name of the mobile configuration that you want to modify.
2. In the Data Sets related list, click **Edit**.
3. From the Data Sets page, you can:
   - Add a data set.
   - Remove a data set by selecting the data set you want to remove and clicking **Remove**.
   - Edit a data set by selecting the data set you want to edit in the hierarchy. The right pane displays the filters for that data set.
   - Test your mobile configuration.

   As you define and modify the data sets, Salesforce automatically saves your changes.
4. Click **Done** when you are finished.

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view mobile data sets:

- View Setup and Configuration

To create, change, or delete mobile data sets:

- Manage Mobile Configurations

Adding Data Sets

To add a data set:

1. In the hierarchy, select **Data Sets** to create a parent data set, or select an existing data set to create a child data set.
2. Click **Add...**.
3. In the popup window, select the object for the records you want the data set to include. Salesforce lets you create parent data sets for all custom objects and the following standard objects:
   - Accounts

- Assets
- Attachments
- Cases
- Contacts
- Content
- Events
- Leads
- Notes
- Opportunities
- Price Books
- Products
- Solutions
- Tasks
- Users

Note:

- Although attachments are available as a data set, they're only supported in Salesforce Mobile Classic for Android.
- Salesforce Mobile Classic supports default field values only for picklists and multiselect picklists. Default field values for other types of fields, such as checkboxes and numeric fields, do not appear in Salesforce Mobile Classic.

When adding to an existing data set, the popup window displays any object with a relationship to the selected object. This includes child objects, and also parent objects with a master-detail or lookup relationship to the selected object.

For example, assume you created an account field called Primary Contact with a lookup relationship to the contact object. If you add Account as a top-level data set in a mobile configuration, you see two sets of contacts when you add Contact below Account:

- **Contact:** Represents the standard relationship between the account and contact objects.
- **Contact (Referenced by Account):** Represents any object that is the parent in a lookup or master-detail relationship for the selected object. In this case, the contact object is referenced by the Primary Contact field on the account object.

Because Salesforce distinguishes between these two types of relationships, you could, for example, mobilize just the contacts referenced by a custom account field without sending any child contact records to the device.

4. Click **OK**. The data set you created appears in the hierarchy.
5. Optionally, use filters to restrict the records that a parent or child data set includes:
   a. Use the Filter by Record Ownership options to configure Salesforce to automatically synchronize records based on the owner of the record. The possible options are:
      - `All Records`: Salesforce automatically synchronizes all records the user can access. The `All Records` option is not available for tasks and events when they are parent data sets in a mobile configuration. This helps prevent failed data synchronization due to activity filter queries that take too long to run.
      - `User's Records`: Salesforce automatically synchronizes all records the user owns.
      - `User's Team's Records`: Salesforce automatically synchronizes all records owned by the user and the user's subordinates in the role hierarchy.
      - `User's Account Team's Records`: Salesforce automatically synchronizes accounts for which the user is an account team member, but does not include accounts owned by the user.

- `User's Opportunity Team's Records`: Salesforce automatically synchronizes opportunities for which the user is an opportunity team member, but does not include opportunities owned by the user.
- `None (Search Only)`: Salesforce does not automatically synchronize any records for this data set; however, users can use their mobile devices to search all of the records they can access.

Salesforce only displays options that relate to the selected data set. For example, selecting an account data set displays the `User's Account Team's Records` option, while selecting an opportunity data set displays the `User's Opportunity Team's Records` option.

If your mobile needs for an object require a combination of the available record ownership filters, you can add the same object data set up to four times on the same hierarchy level. For example, a sales manager might want to synchronize his opportunities, opportunities owned by his subordinates, and opportunities for which he is an opportunity team member. In this case, you would add an opportunity data set and select `User's Team's Records`, then add a second opportunity data set at the same level in the hierarchy and select `User's Opportunity Team's Records`. Note that objects with only one ownership filter option, such as Case Comment, cannot be added multiple times at the same level of the hierarchy.

b. Set the filter criteria to automatically synchronize only records that meet specific criteria in addition to the Filter by Record Ownership option you selected. For example, you can set the filter to only include opportunity records with amounts greater than $50,000, or contact records with the title “Buyer.”

c. To prevent a single data set from consuming all the memory on a mobile device, select the second radio button under Set Max Record Limit and enter the maximum number of records this data set can transfer to mobile devices. Use the Order By and Sort drop-down lists to specify which records are synchronized if the data size limit is exceeded.

If the limit is reached, Salesforce updates the records currently on the mobile device approximately every 20 minutes, and replaces the records approximately every 24 hours in accordance with the Order By and Sort settings. For example, if the settings are Last Modified Date and Descending, Salesforce transfers the most recently modified records to mobile devices and removes the same number of records that were least recently modified.

If you selected the `None (Search Only)` Filter by Record Ownership option, the limit you set does not apply because no records are automatically synchronized.

Tip: Do not use Set Max Record Limit in place of filters. Only use Set Max Record Limit as a safety mechanism, and use filters as the primary means of limiting the number of records on a mobile device. This ensures that your mobile users receive the correct records on their devices.

Because of the memory restrictions of mobile devices, Salesforce prevents a single query from returning more than 2,500 records.

6. Be sure to test your mobile configuration to make sure the data does not exceed the total data size limit.
7. Click **Done**.

SEE ALSO:

Support On-the-Go Productivity with Salesforce Mobile Classic

Manage Salesforce Mobile Classic Configurations

Setting Up Salesforce Mobile Classic

Merge Fields for Mobile Filter Criteria

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

Some of the $User merge fields are available when defining filters for mobile configurations and mobile custom views. In mobile configurations, you can use these merge fields to synchronize records where the user is linked to a record but is not the record owner. For example, you can send cases created by the current user to the mobile device, or you can send records to the device where the current user is referenced in a custom field. In mobile views, you can use the merge fields to define view based on the record owner; for example, you might create a view that displays the current user's accounts with a rating of "Hot".

The following table describes the available user merge fields:

Merge Field	Description
`$User.ID`	References the ID of the current user. This merge field can be applied to fields that contain a user lookup. The valid operators for this merge field are Equals and Not Equal To. When creating mobile view filters that reference an owner field, you can only use the `$User.ID` merge field.
`$User.Username`	References the username of the current user. This merge field can be applied to any text or lookup field, except picklists. The valid operators for this merge field are Equals, Not Equal To, Greater Than or Equal, Less Than or Equal, Contains, Does Not Contain, and Starts With.
`$User.Firstname`	References the first name of the current user. This merge field can be applied to any text or lookup field, except picklists. The valid operators for this merge field are Equals, Not Equal To, Greater Than or Equal, Less Than or Equal, Contains, Does Not Contain, and Starts With.
`$User.Lastname`	References the last name of the current user. This merge field can be applied to any text or lookup field, except picklists. The valid operators for this merge field are Equals, Not Equal To, Greater Than or Equal, Less Than or Equal, Contains, Does Not Contain, and Starts With.
`$User.Fullname`	References the first and last name of the current user. This merge field can be applied to any text or lookup field, except picklists. The valid operators for this merge field are Equals, Not Equal To, Greater Than or Equal, Less Than or

Merge Field	Description
	Equal, Contains, Does Not Contain, and Starts With.

SEE ALSO:

- Manage Salesforce Mobile Classic Configurations
- Support On-the-Go Productivity with Salesforce Mobile Classic
- Define Data Sets

Sample Data Sets

Many administrators create mobile configurations based on the functional groups in their organization because users in the same group usually have similar mobile requirements for data. Below are sample data sets for common Salesforce groups. Your mobile users have unique needs, but you can use the examples as a reference to help you get started with mobile configurations.

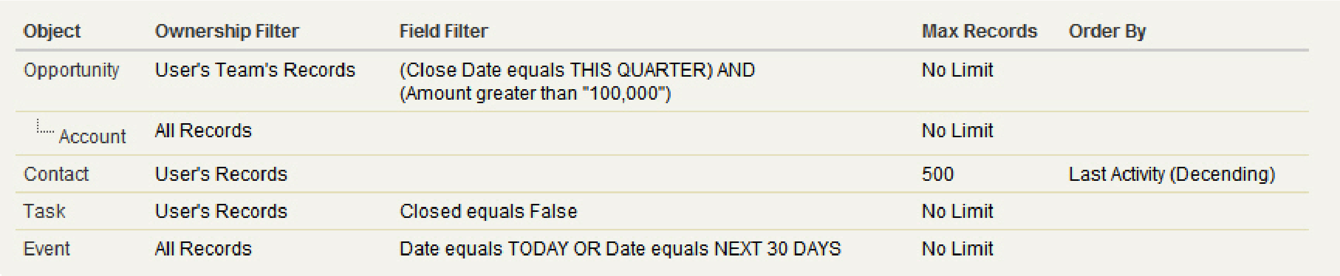
Sales Manager

Sales managers usually need to see records they own and also the records of their subordinates. They also tend to closely monitor large deals in the pipeline.

This mobile configuration allows sales managers to see:

- The opportunities they own.
- The opportunities owned by users who report to them in the role hierarchy.
- All opportunities scheduled to close in the current quarter with an amount greater than $100,000.
- All accounts related to the opportunities.
- A subset of their contact and activity records.

Sample Mobile Configuration for Sales Managers

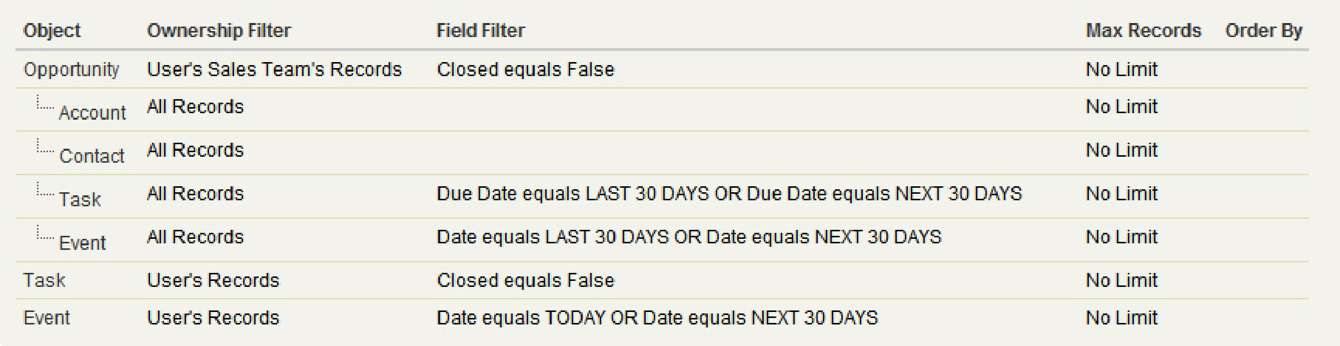


Object	Ownership Filter	Field Filter	Max Records	Order By
Opportunity	User's Team's Records	(Close Date equals THIS QUARTER) AND (Amount greater than "100,000")	No Limit	
Account	All Records		No Limit	
Contact	User's Records		500	Last Activity (Decending)
Task	User's Records	Closed equals False	No Limit	
Event	All Records	Date equals TODAY OR Date equals NEXT 30 DAYS	No Limit	

Sales Engineer

The sales engineer mobile configuration retrieves opportunities owned by the other members of the user's opportunity team, but does not include the user's records. The configuration is opportunity-based because all accounts and contacts sent to the device are related to the opportunities. The sales engineers would see activity history related to the opportunities on the device and also their own activities.

Sample Mobile Configuration for Sales Engineers

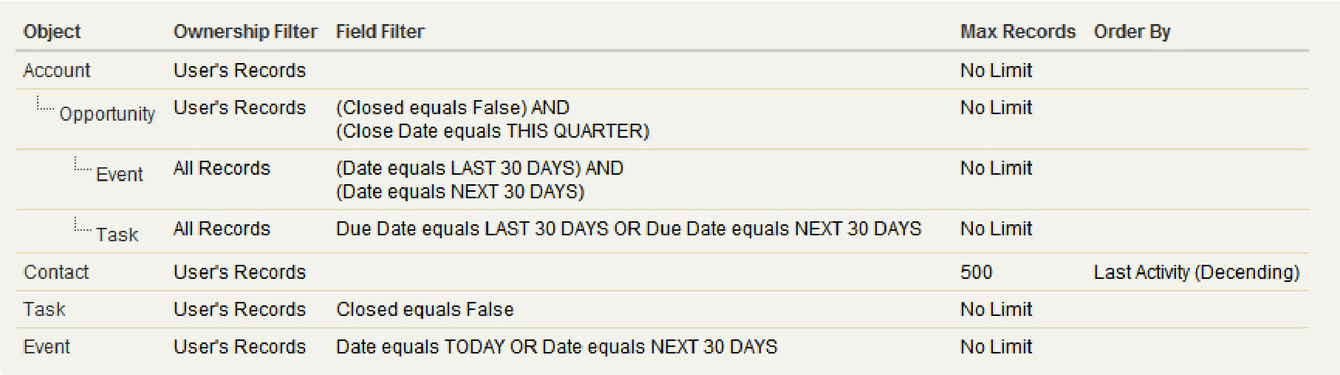


Object	Ownership Filter	Field Filter	Max Records	Order By
Opportunity	User's Sales Team's Records	Closed equals False	No Limit	
└ Account	All Records		No Limit	
└ Contact	All Records		No Limit	
└ Task	All Records	Due Date equals LAST 30 DAYS OR Due Date equals NEXT 30 DAYS	No Limit	
└ Event	All Records	Date equals LAST 30 DAYS OR Date equals NEXT 30 DAYS	No Limit	
Task	User's Records	Closed equals False	No Limit	
Event	User's Records	Date equals TODAY OR Date equals NEXT 30 DAYS	No Limit	

Account Executive

This account executive mobile configuration is account-based, which means the device pulls down the user's accounts and opportunities related to those accounts. The opportunities are filtered so that only open opportunities scheduled to close in the current quarter appear on the device. The Task and Event child data sets retrieve all activities related to those opportunities, not just the user's activities. Only open tasks and events from a two-month window are sent to the device. The Task and Event parent data sets pull down just the user's activities and restrict the activities to open tasks and events scheduled for the next 30 days. The Contact data set delivers the user's contact records, but limits the record count to the 500 most recently active contacts.

Sample Mobile Configuration for Account Executives

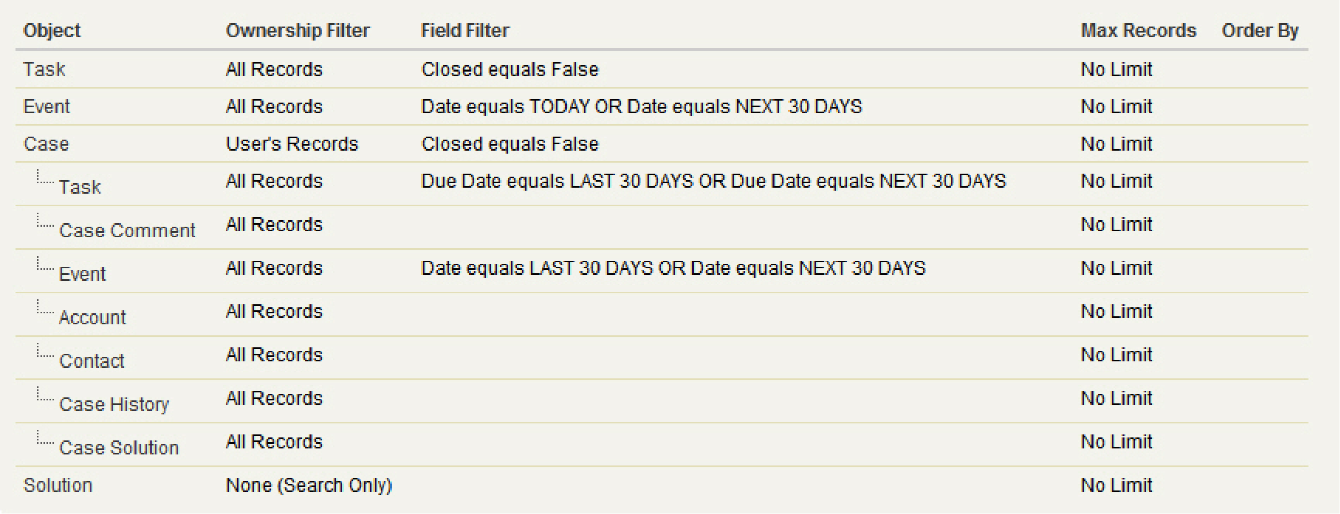


Object	Ownership Filter	Field Filter	Max Records	Order By
Account	User's Records		No Limit	
└ Opportunity	User's Records	(Closed equals False) AND (Close Date equals THIS QUARTER)	No Limit	
└ Event	All Records	(Date equals LAST 30 DAYS) AND (Date equals NEXT 30 DAYS)	No Limit	
└ Task	All Records	Due Date equals LAST 30 DAYS OR Due Date equals NEXT 30 DAYS	No Limit	
Contact	User's Records		500	Last Activity (Decending)
Task	User's Records	Closed equals False	No Limit	
Event	User's Records	Date equals TODAY OR Date equals NEXT 30 DAYS	No Limit	

Customer Support Representative

Customer support representatives are focused primarily on cases and solutions. This mobile configuration delivers all open cases to the user's device, along with related accounts, contacts, case comments, case history, tasks, and events. The Case Solution child data set sends all solutions related to the cases, and the Solution data set lets the user search for solutions from the Solutions tab on the device. The support representatives also have access to a subset of their activity records.

Sample Mobile Configuration for Customer Support Representatives



Object	Ownership Filter	Field Filter	Max Records	Order By
Task	All Records	Closed equals False	No Limit	
Event	All Records	Date equals TODAY OR Date equals NEXT 30 DAYS	No Limit	
Case	User's Records	Closed equals False	No Limit	
└ Task	All Records	Due Date equals LAST 30 DAYS OR Due Date equals NEXT 30 DAYS	No Limit	
└ Case Comment	All Records		No Limit	
└ Event	All Records	Date equals LAST 30 DAYS OR Date equals NEXT 30 DAYS	No Limit	
└ Account	All Records		No Limit	
└ Contact	All Records		No Limit	
└ Case History	All Records		No Limit	
└ Case Solution	All Records		No Limit	
Solution	None (Search Only)		No Limit	

SEE ALSO:

Support On-the-Go Productivity with Salesforce Mobile Classic

Manage Salesforce Mobile Classic Configurations

Define Data Sets

Test Salesforce Mobile Classic Configurations

When you create a Salesforce Mobile Classic configuration, you specify a total data size limit for the configuration. The total data size limit prevents Salesforce from sending too much data to the mobile devices of users assigned to the mobile configuration. After defining the data sets, it’s important to test the mobile configuration to make sure the total data size limit isn’t exceeded.

To estimate the size of the data set that the mobile configuration will deliver to a user's device:

1. From Setup, enter `Salesforce Classic Configurations` in the `Quick Find` box, then select **Salesforce Classic Configurations**. Then click the name of the mobile configuration that you want to test.
2. In the Data Sets related list, click **Edit**.
3. In the Test Data Size section, click the lookup icon next to the `Select a user` field to choose the user you want to test. While users must be mobile-enabled in order to assign them to mobile configurations, you can test the configuration's data size against any user account.

   The `Select a user` field defaults to the name of the user currently logged in; however, it is important to test a mobile configuration with the accounts of users who will actually be assigned to the configuration, particularly users who own a large number of records.

4. Select the **Include metadata** checkbox to include metadata in the estimate. Metadata consists of page layout and schema information, and the amount of metadata sent to a device can be very high depending on the size of your organization and the complexity of its setup.

   Warning: It might take a while for Salesforce to calculate the metadata size in addition to the data size. Even if you choose to hide the metadata in your test results, the metadata is still factored into the total data size when the mobile device synchronizes with Salesforce.

5. Click **Estimate Data Size**.

   The size of each data set is calculated. Results display in the hierarchy tree, which is the left pane of the data set region at the top of the page. Additional results appear in the Test Data Size section below the hierarchy.

   - In the hierarchy tree, two numbers appear next to each data set. The first represents the number of records generated by the data set, and the second represents the total size of the data set in bytes or kilobytes. This breakdown is useful for identifying which data sets might require additional filtering criteria to reduce the size.
   - The Test Data Size section provides an estimate of the data that the current mobile configuration would deliver to the selected user's device, including:
     - The size and number of records in each object's data set.
     - The total size and number of records, which includes records in the data set and marked records. A marked record is a record that is not part of a user's mobile configuration. There are two ways marked records can become part of the data set:
       - The user downloads records to his or her device through online searches, and the records are flagged so that they get sent to the user's device every time the device synchronizes with Salesforce.
       - Records in the user's data set contain lookup fields to records that do not match the mobile configuration's filter criteria. Salesforce synchronizes the records referenced in the lookup fields so that users do not encounter broken links in the mobile app.

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter ’17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter ’17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic data sets:

- View Setup and Configuration

To test Salesforce Mobile Classic configurations:

- Manage Mobile Configurations

Tip: For an accurate count of the marked records, synchronize the data in the mobile app before estimating the data size. To synchronize the data:

- On an Android device, tap **Application Info** > **Sync Now** > **Refresh All Data**.
- On an iPhone device, tap **More**, then tap **App Info**. Tap **Sync Now**, then tap **Refresh All Data**.

- The size of the metadata that would be sent to the device for the user, if you selected the **Include metadata** checkbox.
- The total mobilized data set, which is the sum of all the records.

- Reports are not included in the data size estimate.

6. Compare the test results to the total data size limit that was set for the configuration; the limit is located in the top of the Test Data Size section. Click the size limit to increase or decrease the value on the Edit Mobile Configuration page.
   - If the total data size is below the limit, the selected user can safely be assigned to the mobile configuration. However, keep in mind that the test results are an estimate because different devices have different storage algorithms.
   - If the total data size exceeds the limit, reduce the size of the data by reducing the scope of your data set, refining the filter criteria of your data sets, deleting a data set, or removing fields from the mobile page layout. Repeat the testing process until the data is below the total limit.

   Note: The data size estimate in the Test Data Size section does not automatically refresh if you edit the data sets. Click **Refresh Data Size** to update the test results.

SEE ALSO:

Support On-the-Go Productivity with Salesforce Mobile Classic

Manage Salesforce Mobile Classic Configurations

Manage Salesforce Mobile Classic Devices

Setting Up Salesforce Mobile Classic

Edit Object Properties for Salesforce Mobile Classic

You can change the properties of standard and custom objects in the Salesforce Mobile Classic app. For example, you can restrict the permissions of Salesforce Mobile Classic users, or you can exclude unnecessary fields from the object's mobile page layout.

Salesforce Mobile Classic object properties are customized per mobile configuration. To edit mobile object properties:

1. From Setup, enter `Salesforce Classic Configurations` in the `Quick Find` box, then select **Salesforce Classic Configurations**.
2. Click the name of the mobile configuration you want to modify.
3. In the Mobile Object Properties related list, click **Edit** next to an object name.

   Only objects you mobilized in the configuration's data set appear in the related list. You can't change the properties of the user object.

4. From the Edit Mobile Configuration page, you can:
   - Remove Mobile Permissions
   - Customize Salesforce Mobile Classic Page Layouts
5. Click **Save**.

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic configurations:

- View Setup and Configuration

To edit Salesforce Mobile Classic object properties:

- Manage Mobile Configurations

Remove Mobile Permissions

The Salesforce Mobile Classic app inherits the user's permissions from Salesforce. Some administrators want to further restrict the permissions of users when they access Salesforce data in Salesforce Mobile Classic, usually due to limitations of the app or the possibility of user error. For example, users can inadvertently delete a record because they don't realize that deleting a record in Salesforce Mobile Classic also deletes the record in Salesforce. If this is a concern, administrators can prevent users from deleting records in the mobile application, regardless of their standard and custom object permissions in Salesforce. Also, Salesforce Mobile Classic doesn't support all Salesforce features, such as S-controls and Apex. If your business process for an object is unsupported by Salesforce Mobile Classic, you might choose to prevent mobile users from updating those records in the app.

In the Permissions section, select which permissions to remove from mobile users for this object. Use the **Deny Create**, **Deny Edit**, or **Deny Delete** checkboxes to prevent users from creating, editing, or deleting records in Salesforce Mobile Classic.

Note: Currently, you can't block mobile permissions for the content object.

Customize Salesforce Mobile Classic Page Layouts

The Salesforce Mobile Classic app inherits the user's page layouts from Salesforce. Administrators may want to exclude some fields from each object's mobile page layout because unnecessary fields consume memory and make it harder for users to scroll through pages on the mobile device.

In the Excluded Fields section, select which fields to display on the mobile device for this object. To add or remove fields, select a field name, and click the **Add** or **Remove** arrow.

- Administrators can view all available fields per object, regardless of field-level security.

- Certain fields are required in order for Salesforce Mobile Classic to communicate with Salesforce. Those fields don't display in the Available Fields box because they are mandatory and can't be excluded from mobile page layouts.
- Fields used in custom mobile views can't be excluded from mobile page layouts.
- If you mobilize the content object, all of the content object's fields display in the Available Fields box; however, the layout of the content detail page in the Salesforce Mobile Classic app is hard-coded to show only a few fields. Excluding fields for the content object doesn't affect the page layout in the app.

SEE ALSO:

Support On-the-Go Productivity with Salesforce Mobile Classic
Manage Salesforce Mobile Classic Configurations
Manage Salesforce Mobile Classic Tabs
Create Links to Web and Visualforce Mobile Pages for Salesforce Mobile Classic
Setting Up Salesforce Mobile Classic

Assign Tabs to a Salesforce Mobile Classic Configuration

For each mobile configuration, you can select the tabs that appear in the Salesforce Mobile Classic app and define the order of the tabs. The available tabs for a mobile configuration include:

- Standard object tabs
- Custom object tabs
- Visualforce and web tabs that have been enabled for Salesforce Mobile Classic

> Warning: Not all websites and Visualforce features are supported on mobile devices. Carefully review the best practices for creating mobile-friendly pages before enabling Visualforce or web tabs for the Salesforce Mobile Classic app.

By default, tabs work the same in the Salesforce Mobile Classic app as in the full Salesforce site—if an object's tab is hidden in Salesforce, it's hidden in Salesforce Mobile Classic as well.

> Note: If you customize mobile tabs, the tabs you select for the mobile configuration are sent to users' mobile devices even if the tabs have not been added to a configuration. Although the tabs are sent to the device, they only display in the Salesforce Mobile Classic app if users have permission to view the tab.

There are several reasons you might want to hide an object's tab in Salesforce Mobile Classic even though the object records are sent to the device. The Salesforce Mobile Classic app has much less screen space to display a row of tabs, so occasionally you might choose to reduce the number of tabs on the device. Also, sometimes a custom object has a relationship to a standard object, and users access the custom object record from the parent object record. In that case, you could mobilize the custom object but hide the tab.

To assign tabs to a mobile configuration:

1. From Setup, enter `Salesforce Classic Configurations` in the `Quick Find` box, then select **Salesforce Classic Configurations**. Then click the name of a mobile configuration.
2. In the Mobile Tabs related list, click **Customize Tabs** to define mobile tabs for the first time. If you have already set up the mobile tabs, click **Edit**.

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic configurations:
- View Setup and Configuration

To customize Salesforce Mobile Classic tabs:
- Manage Mobile Configurations

3. Select tabs from the `Available Tabs` list, and click the **Add** arrow to add them to the mobile configuration.
4. In the `Selected Tabs` list, choose tabs and click the **Up** and **Down** arrows to arrange the tabs in the order they should appear in the Salesforce Mobile Classic app.
5. Click **Save**.

Note: iPhone users can customize the order of their tabs in the Salesforce Mobile Classic app. If the user customizes their tab order, any administrator changes to the tab order in the mobile configuration are ignored by the app, and any newly mobilized tabs are added below the user's existing tabs.

SEE ALSO:

Manage Salesforce Mobile Classic Tabs

Enabling Web and Visualforce Tabs for Salesforce Mobile Classic

Support On-the-Go Productivity with Salesforce Mobile Classic

Manage Salesforce Mobile Classic Configurations

Enabling Web and Visualforce Tabs for Salesforce Mobile Classic

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

You can make web and Visualforce tabs available in the Salesforce Mobile Classic app. When you build the web tab or Visualforce tab, edit the tab properties and select the `Salesforce Mobile Classic Ready` checkbox to ensure that the web page or Visualforce page displays and functions properly on a mobile device. Selecting the checkbox adds the tab to the list of available tabs for your Salesforce Mobile Classic mobile configurations.

It is important to note that most mobile browsers have technical limitations concerning display size, scripts, processor speed, and network latency. Review the following considerations before mobilizing your web and Visualforce pages to ensure that they are compatible with mobile browsers.

Mobile Web Tab Considerations

Consider the following when defining a web tab that will be used in the Salesforce Mobile Classic app:

- The ability to mobilize web tabs is only available for iPhone devices. If you mobilize a web tab, keep in mind that Android users can't view the tab in Salesforce Mobile Classic.
- The tab type must be URL. The mobile application can't run S-controls.
- Some web pages contain JavaScript and Flash, but not all mobile browsers support them:
  - Apple's Safari browser supports JavaScript, but not Flash.
- Before mobilizing a web tab, navigate to the target URL on one of your organization's mobile devices to verify that it works as expected in a mobile browser. In the event that your organization's device inventory includes phones with different operating systems—for example, iPhone devices—be sure to test on each type of device. If users can't accomplish the necessary tasks on the web page from a mobile browser, do not mobilize the web tab.

Visualforce Mobile Tab Considerations

Consider the following when defining a mobile Visualforce tab:

- Visualforce Mobile is only available for iPhone. If you mobilize a Visualforce tab, keep in mind that Android users can't view the tab in Salesforce Mobile Classic.

- Because the display size is limited on mobile browsers, we recommend redesigning the Visualforce page to optimize it for mobile users:
  - Set the `sidebar` and `showHeader` attributes on the `<apex:page>` tag to `false`. Phones have small screens and limited processing power, so it is essential that the page suppresses the tab header and sidebar.
  - Set the `standardStylesheets` attribute on the `<apex:page>` tag to `false`. The standard Salesforce style sheet causes pages to load slowly on the device. The best approach to adding a style sheet to your page is to include a `<style>` section just below the `<apex:page>` component.
  - Set the `columns` attribute on the `<apex:pageBlockSection>` component to `1`. There is not enough room on a mobile device's screen to display two columns, so specifying a one-column layout prevents fields from wrapping awkwardly on the page.
- Splash pages don't display in the Salesforce Mobile Classic app.
- In the Salesforce Mobile Classic app, the Visualforce page is embedded in a tab, so you should avoid using tabs for navigation in mobile Visualforce pages.
- Even if you know that the mobile browser supports the JavaScript in your Visualforce page, keep your use of JavaScript to a minimum. Mobile devices generally have slow network connections, and too many scripts running on a page creates a poor user experience. To minimize the amount of JavaScript on your mobile Visualforce pages, try to build them using mostly HTML.
- All Visualforce pages contain JavaScript, even if you don't create pages that use JavaScript code.
- User agent inspection can be executed in a custom controller to support multiple devices. You can do this by inspecting the appropriate result of the `getHeaders()` method on the current page reference.

SEE ALSO:

Manage Salesforce Mobile Classic Tabs

Manage Salesforce Mobile Classic Configurations

Create Links to Web and Visualforce Mobile Pages for Salesforce Mobile Classic

Assign Tabs to a Salesforce Mobile Classic Configuration

Create List Views for Salesforce Mobile Classic

You can create custom list views for Salesforce Mobile Classic users. Custom list views for Salesforce Mobile Classic, also called mobile views, are different from Salesforce custom views in these ways:

- Administrators set up mobile views for each mobile configuration. The views are available to all users assigned to the configuration, and administrators can't restrict visibility to certain groups of users within the configuration. Each mobilized object in a mobile configuration can have up to 10 custom views.
- Users can't filter mobile views by All Records or My Records. The views apply to all records stored locally on the device regardless of ownership; however, ownership filters can be applied using the additional fields in the search criteria.
- Mobile views don't support filter logic.
- Mobile views are limited to a two-column display.
- Users can sort mobile views in ascending or descending order by up to two fields.

For each mobile configuration, you can define up to 10 custom views per object. These views are then pushed to the devices of users assigned to the affected configurations. To create a custom view for Salesforce Mobile Classic:

1. From Setup, enter `Salesforce Classic Configurations` in the `Quick Find` box, then select **Salesforce Classic Configurations**. Then click the name of a mobile configuration. You might need to create a mobile configuration if you haven't already.
2. Scroll down to the Mobile Views related list.
3. Choose an object type from the Select an object drop-down list, and then click **New Mobile View**. Only objects included in the mobile configuration's data set appear in the drop-down list. You can't create mobile views for the user object.
4. Enter the view name.

   Because display space on mobile devices is limited, the maximum length of a mobile view name is 30 characters.
5. In the Specify Filter Criteria section, enter conditions that the selected items must match; for example, *`Amount is greater than $100,000`*.
   a. Choose a field from the first drop-down list.

      Note: You can't create views based on fields you excluded from mobile page layouts or fields that are hidden for all profiles and permission sets.

   b. Choose a filter operator.
   c. In the third field, enter the value to match.

      Warning: Note the following about filter criteria values for mobile views:

      - You can use the `$User.ID` merge field as a value in your filter criteria to reference the current user. You can't enter user names in your filter criteria.
      - You can only enter special date values in your filter criteria, not actual dates.
      - You can't use FISCAL special date values in the filter criteria.

   d. Select **Match All** if items in the mobile view should match all the criteria you entered. Select **Match Any** if items in the mobile view should match any of the criteria you entered. Mobile custom views do not support advanced filtering options.

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic devices and users:

- View Setup and Configuration

To manage Salesforce Mobile Classic custom views:

- Manage Mobile Configurations

6. In the Select Fields to Display section, select the fields to use as display columns.

   The default fields are automatically selected. You can choose up to two different columns of data fields to display in your mobile custom view.

7. In the Define Sort Order section, optionally set a primary and secondary sort order for the view.
   1. Select a field in the Order By drop-down list. You can sort by fields that have been excluded from the object's mobile page layout.
   2. Set the sort order to Ascending or Descending.

8. Click **Save**.

SEE ALSO:

Manage Salesforce Mobile Classic Views

Manage Salesforce Mobile Classic Configurations

Manage Salesforce Mobile Classic Devices

Setting Up Salesforce Mobile Classic

Enable Reports in Salesforce Mobile Classic

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To create, edit, and delete public report folders:

- Manage Public Reports

To view Salesforce Mobile Classic configurations:

- View Setup and Configuration

To enable reports in the Salesforce Mobile Classic app:

1. Create a Mobile Reports folder in Salesforce. From the reports home page in the full site, click **Create New Folder**.
2. In the `Report Folder` field, enter: *`Mobile Reports`*.

   The server won't load reports on mobile devices unless this folder is named `Mobile Reports`. Be sure to check for any typos in the name before saving the folder. Additionally, Salesforce doesn't require folder names to be unique. Salesforce Mobile Classic users can see any report stored in all folders named Mobile Reports unless you restrict access with the folder visibility option.
3. Choose a `Public Folder Access` option. This option doesn't affect the ability of mobile users to run reports.
4. Optionally, select any unfiled reports and click **Add** to store them in the Mobile Reports folder. You can also add reports to the folder after saving the folder.
5. Choose a folder visibility option.
   - `This folder is accessible by all users` gives every user in your organization the ability to see the list of mobile reports from their devices.
   - `This folder is accessible only by the following users` lets you grant access to a desired set of users.

     Don't make the `Mobile Reports` folder private unless you want to hide mobile reports from all users, including yourself.
6. Click **Save**.
7. Add reports to the Mobile Reports folder. Click the report name on the reports home page, then click **Save As** and save the report in the Mobile Reports folder.

   After saving the report, you can edit the options to make the report easier to view on a mobile device. For example, you might reduce the number of columns or enter additional filtering criteria.
8. Add the Reports tab to your mobile configurations. From Setup, enter *`Salesforce Classic Configurations`* in the `Quick Find` box, then select **Salesforce Classic Configurations**. Then click the name of a mobile configuration.
9. In the Mobile Tabs related list, click **Customize Tabs** to define mobile tabs for the first time. If you've already set up the mobile tabs, click **Edit**.
10. Select **Reports** from the Available Tabs list, then click the **Add** arrow to add it to the mobile configuration. The Available Tabs list includes standard object tabs and custom object tabs. It can also include web and Visualforce tabs.

    Warning: If you have not yet customized tabs in the mobile configuration, you must select all the tabs that should appear in the Salesforce Mobile Classic, not just the Reports tab.
11. In the Selected Tabs list, choose the Reports tab and click the **Up** and **Down** arrows to define where the Reports tab should appear in the Salesforce Mobile Classic app.
12. Click **Save**.

Note: Currently, reports in Salesforce Mobile Classic aren't available on Android or iPhone devices.

SEE ALSO:

Setting Up Salesforce Mobile Classic

Set Up Salesforce CRM Content for Salesforce Mobile Classic

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic configurations:

- View Setup and Configuration

To create, change, or delete Salesforce Mobile Classic data sets:

- Manage Mobile Configurations

Note the following about how Salesforce CRM Content is implemented in Salesforce Mobile Classic:

- Content record information is synchronized to the device; however, the files associated with the content records are not. This allows users to deliver content from the app even when a file is too large to be downloaded to a mobile device.
- Users can't search for a specific piece of content in the app. They can only share the content available on the Content tab, which is automatically synchronized to their device based on the filters in their assigned mobile configuration.
- Users can't view a list of their subscribed content in the app. They also can't filter the list of records on the Content tab based on a particular library.
- While users can preview and share content from the app, they can't update the file associated with a content record. If they have the required permissions, they can edit the fields on the content detail page.
- Users must have a data connection to preview and deliver content. Without a data connection, they can only view the content detail page.
- Content in Salesforce Mobile Classic is only supported on iPhone devices.
- You can't block mobile permissions for the content object. Currently, the content object in Salesforce Mobile Classic is read-only.
- You can't edit the mobile page layout for the content object. The content detail page in the app is hard-coded to display only a few fields.

To set up Content for a Salesforce Mobile Classic configuration:

1. From Setup, enter *`Salesforce Classic Configurations`* in the `Quick Find` box, then select **Salesforce Classic Configurations**, and then click the name of a mobile configuration.
2. In the Data Sets related list, click **Edit**.
3. Click **Add...**.
4. In the popup window, select Content, then click **OK**.
5. Use field filters to specify which content records are synchronized.

   Because users can't search for content in the Salesforce Mobile Classic app, it's essential to set up filters that make important content available on the device. You can't create filters based on libraries or subscriptions, but here are a few options for setting up useful filter conditions:

   - **Date:** Filter on the `Last Modified Date`, `Content Modified Date`, or `Created Date` fields. Use special date values like LAST 90 DAYS or LAST 180 DAYS to ensure that recently updated content records are synchronized.
   - **Owner:** Filter on the author if certain people in your organization are responsible for publishing content.
   - **File Type:** Filter on certain types of documents. For example, your opportunity team might generally be interested in presentations or PDF documents.

- **Custom Fields:** If you created custom content fields that help you categorize your content, filter on the custom fields. For example, if you built a `Functional Use` field with picklist values, you could set up a filter condition where `Functional Use` equals *`Sales`*.

6. Optionally, prevent content records from consuming all the memory on a mobile device by selecting the second radio button under Set Max Record Limit and entering the maximum number of content records this configuration can transfer to mobile devices. Use the Order By and Sort drop-down lists to specify which records are synchronized if the data size limit for your mobile configuration is exceeded.
7. Click **Done**.

SEE ALSO:

Setting Up Salesforce Mobile Classic

Configuring Salesforce Mobile Classic Access for Partner Users

Note: Starting in Summer '13, the partner-portal is no longer available for organizations that aren't currently using it. Existing organizations continue to have full access. If you don't have a partner-portal, but want to easily share records and information with your partners, try Communities.

Existing organizations using partner-portals may continue to use their partner-portals or transition to Communities. Contact your Salesforce Account Executive for more information.

You can allow partner users to access partner portal data on mobile devices using the Salesforce Mobile Classic app.

Tips for setting up Salesforce Mobile Classic access for partner users:

- Before setting up Salesforce Mobile Classic for partner users, you must configure partner user accounts and purchase mobile licenses for each partner portal user that will be using Salesforce Mobile Classic. Partner user profiles must be assigned to at least one active partner portal before partner users can use Salesforce Mobile Classic. If a user profile is assigned to multiple partner portals, only the first assigned partner portal will be accessible using Salesforce Mobile Classic.
- Custom mobile list views don't affect list views in the partner portal.
- If you make User data sets available in the Salesforce Mobile Classic app, partners can assign objects to their partner account users and all internal users. If you don't make User data sets available, partners can only assign objects to internal or partner account users who are associated with records that you've made available on the mobile device.

SEE ALSO:

Setting Up Salesforce Mobile Classic

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic configurations, data sets, mobile devices, and users:

- View Setup and Configuration

To create, change, or delete Salesforce Mobile Classic configurations and data sets, test mobile configurations, edit mobile object properties, and manage mobile custom views:

- Manage Mobile Configurations

Create Links to Web and Visualforce Mobile Pages for Salesforce Mobile Classic

To improve the integration between the Salesforce Mobile Classic app, Visualforce Mobile, and external websites, you can optionally create links from native Salesforce records to Visualforce Mobile pages or external websites. To create the links, build text formula fields on a standard or custom object. The field must be visible on the page layout to appear in the Salesforce Mobile Classic app. The best practice is to include all embedded links in a separate section labeled "Mobile Links" at the bottom of the page layout. There is currently no way to hide these links in Salesforce, but users can collapse the section to keep the links out of the way.

1. Navigate to the fields area of the appropriate object.
2. Click **New** in the fields section of the page.
3. Select `Formula`, and then click **Next**.
4. Enter the field label.

   The field name is automatically populated based on the field label you enter.

5. Select `Text`, then click **Next**.
6. In the formula editor, create the link to the custom Visualforce page or external website:
   - To create a Visualforce link, type *`"visualforce:///apex/PageName"`*, and replace *`PageName`* with the name of your Visualforce page. You can append parameters to the string, such as *`?contactid=" & Id"`*, in order to pass information from the record in the client application to the Visualforce page.
   - To create a Web link, type *`"weblink:"`*, followed by the URL to which you want the link to point, such as *`"weblink:http://www.salesforce.com"`*. You can append parameters to the string in order to pass information from the record in the client application to the Web page. For example, the following Web link launches a social networking site from a contact record and performs a search for the contact:

   ```
   "weblink:http://m.linkedin.com/members?search_term=" &FirstName& "+" &LastName&
   "&filter=name&commit=Search"
   ```

   Note: The client application passes the Visualforce or Web link with all parameters to the embedded browser. It is up to the website or Visualforce Mobile page to interpret any parameters. Be sure to construct your Visualforce Mobile page to consume any parameters passed in the link.

7. Click **Next**.
8. Set the field-level security to determine whether the field should be visible or read only for specific profiles, and click **Next**.
9. Choose the page layouts that should display the field. In the next step, you will customize the layout to change the location of the field on the page.
10. Save your changes.
11. Edit the object's page layout. From the management settings for the object whose page layout you want to change, go to Page Layouts.
12. Drag a Section element from the palette to the page layout and drop it below the existing sections.
13. In the `Section Name` field, type *`Mobile Links`*.
14. Deselect the `Edit Page` option.

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To create or change custom buttons or links:
- Customize Application

15. Select the 1-column layout, then click **OK**.

16. Drag the new text formula field from its current location into the new Mobile Links section.

17. Save your changes.

SEE ALSO:

Setting Up Salesforce Mobile Classic

Find Object Management Settings

Notifying Users about Salesforce Mobile Classic Availability

When you're ready to deploy the Salesforce Mobile Classic app to your users, send them an email to notify them about the availability of the app and provide installation instructions. You can send the email using your corporate email application, like Outlook, or you can send mass email from Salesforce. Either way, include the URL that launches the download.

- For Android users, the download URL is `mobile.salesforce.com`. The link is the same for the initial download and for subsequent upgrades.
- You can obtain the iPhone download URL from iTunes. Open iTunes, click **iTunes Store**, then search for Salesforce Mobile Classic. Click the app icon to view details about the app. At the top of the iTunes window is a bread crumb path representing the application's location in the App Store: **App Store** > **Business** > **Salesforce Mobile Classic**. Drag-and-drop the path into a text editor or word processing program to display the app's download URL.

To send mass email to Salesforce Mobile Classic users from Salesforce:

1. Create an email template that informs users about the availability of Salesforce Mobile Classic. From your personal settings, enter *`Templates`* in the `Quick Find` box, and select either **My Templates** or **Email Templates**—whichever one appears. Optionally, you can also create a separate email template for upgrade notifications. Include the download link in the templates.
2. Create a custom view on the Mass Email page that shows your Salesforce Mobile Classic users only.
3. Send mass email to your Salesforce Mobile Classic users, using the custom view that you created. From Setup, enter *`Mass Email Users`* in the `Quick Find` box, then select **Mass Email Users**.

SEE ALSO:

Setting Up Salesforce Mobile Classic

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To create HTML email templates:

- Edit HTML Templates

To send mass emails to users:

- Mass Email

  AND

  Manage Users

Salesforce Mobile Classic FAQ for Administrators

- Is the Salesforce Mobile Classic app secure?

Is the Salesforce Mobile Classic app secure?

All data transmitted between Salesforce and Salesforce Mobile Classic is fully encrypted and secured over the air.

The mobile application has multiple layers of security at the device level. Device venders provide the ability to set password or passcode access restrictions. Users must be required to use the device protection in accordance with your organization's security policy. If the device is locked by password, it is difficult for unauthorized persons to obtain sensitive data.

Additionally, a user must have valid Salesforce credentials to activate the mobile application on the device. When a user registers a new wireless device, the Salesforce data on their old wireless device is automatically erased—users can only activate one mobile device at a time. Users are also warned when a new device is activated using their Salesforce account. If a logged in user exceeds the administrator-configured inactivity period on the mobile device, the mobile session is terminated and the password or passcode is required to reestablish the session.

Administrators can also remotely delete data from any lost or stolen devices.

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

Manage Salesforce Mobile Classic Configurations

To manage your Salesforce Mobile Classic configurations, from Setup, enter `Salesforce Classic Configurations` in the `Quick Find` box, then select **Salesforce Classic Configurations**.

- To define a new mobile configuration, click **New Mobile Configuration**.
- To modify a mobile configuration—including assigning different users or profiles and changing the maximum size of data sets—click **Edit**.
- To activate a mobile configuration, click **Edit**, select the `Active` checkbox, then click **Save**. Deselect `Active` to deactivate the mobile configuration.
- To delete a mobile configuration, click **Del**.
- To view details about a mobile configuration, click its name.

  From a mobile configuration detail page, you can:

  - Modify data sets for a mobile configuration by clicking **Edit** in the Data Sets related list.
  - Change the properties of mobilized objects by clicking **Edit** next to an object name in the Mobile Object Properties related list.
  - Customize mobile configuration tabs by clicking **Edit** in the Mobile Tabs related list.
  - Create custom views for a mobile configuration by clicking **Edit** in the Mobile Views related list.
  - Clone the mobile configuration by clicking **Clone**.

SEE ALSO:

Support On-the-Go Productivity with Salesforce Mobile Classic

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic configurations:

- View Setup and Configuration

To create, change, or delete Salesforce Mobile Classic configurations:

- Manage Mobile Configurations

Salesforce Mobile Classic Permissions

A mobile license is required for each user who will access the Salesforce Mobile Classic app. You allocate mobile licenses using the `Mobile User` checkbox on the user record.

For organizations using Unlimited, Performance, and Developer Editions, Salesforce provides a mobile license for each Salesforce license and the `Mobile User` checkbox is enabled by default for all users. Organizations using Professional or Enterprise Editions must purchase mobile licenses separately and allocate them manually.

Note: The `Mobile User` checkbox is disabled by default for new Performance Edition users.

To prevent users from activating Salesforce Mobile Classic on their mobile devices before you're ready to deploy the app, disable the `Mobile User` checkbox for all your users.

SEE ALSO:

Support On-the-Go Productivity with Salesforce Mobile Classic

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic configurations:

- View Setup and Configuration

To create, change, or delete Salesforce Mobile Classic configurations:

- Manage Mobile Configurations

Manage Salesforce Mobile Classic Tabs

To manage the tabs for a Salesforce Mobile Classic configuration, from Setup, enter `Salesforce Classic Configurations` in the `Quick Find` box, then select **Salesforce Classic Configurations**. Then click the name of the mobile configuration and scroll down to the Mobile Tabs related list.

If you've already customized the configuration's tabs, the Mobile Tabs related list shows the selected tabs.

- To change the tab setup, click **Edit**.
- To delete the mobile tab setup and use the default tab behavior instead, click **Reset to Default**.

If you haven't customized the configuration's tabs, the related list indicates that the default tab behavior is used for the configuration. To customize the tabs used by the configuration and define their order, click **Customize Tabs**.

SEE ALSO:

Support On-the-Go Productivity with Salesforce Mobile Classic

Manage Salesforce Mobile Classic Configurations

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic configurations:

- View Setup and Configuration

To manage Salesforce Mobile Classic tabs:

- Manage Mobile Configurations

Manage Salesforce Mobile Classic Views

To manage the custom views for a Salesforce Mobile Classic configuration, from Setup, enter *Salesforce Classic Configurations* in the `Quick Find` box, then select **Salesforce Classic Configurations**. Then click the name of the mobile configuration and scroll down to the Mobile Views related list.

- To see a list of all your custom views, choose All Objects in the `Select an object` drop-down list. You can also use the Select an object drop-down list to filter the views by object type.
- To create a new mobile view, select the object type from the Select an object drop-down list, and then click **New Mobile View**.
- To make changes to a custom mobile view, click **Edit** next to the view name.
- To delete a mobile custom view, click **Del** next to the view name.
- To view details about a mobile custom view, click its name.

SEE ALSO:

Support On-the-Go Productivity with Salesforce Mobile Classic

Manage Salesforce Mobile Classic Configurations

Manage Salesforce Mobile Classic Devices

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic devices and users:

- View Setup and Configuration

To manage Salesforce Mobile Classic custom views:

- Manage Mobile Configurations

Salesforce Mobile Classic Usage Data in Custom Report Types

You can create custom report types with data that shows how your organization uses Salesforce Mobile Classic. For example, the reports can show how often users access Salesforce Mobile Classic, which mobile device models they use, and so forth.

To create a custom report type with Salesforce Mobile Classic usage data, select the Mobile Session `Primary Object` when defining a custom report type. When you select the fields for the custom report type, choose from the following Salesforce Mobile Classic-specific fields.

Mobile Usage Data Point	Definition
Brand	Wireless carrier
Data Size (Bytes)	Total size of records on device
Device Address	Unique physical address of device (UDID for iOS)
Device Application Version	Installed version of Salesforce Mobile Classic
Device Model	Model of device
Device Operating System Version	Version of operating system installed on device
Duration	Duration of the mobile session in seconds
Last Registration Date	Date of last registration or activation
Last Status Date	Date of last communication received from device
Manufacturer	Manufacturer of device
Metadata Size (Bytes)	Size of metadata (page layouts, picklist values, and so forth) on the device
Owner: Full Name	Name of the device user
Session Start Date	Date the mobile session started
Status	Indicator that the user's data set exceeds the maximum allowed size by the mobile configuration

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To create or update custom report types:

- Manage Custom Report Types

To delete custom report types:

- Modify All Data

Note:

- Mobile sessions are similar to Web-based sessions in login history reports; however, mobile sessions have a fixed timeout value of 20 minutes. Salesforce creates a new Mobile Session when a user logs into or launches Salesforce Mobile Classic after 20 minutes of inactivity in the app or on the device in general.
- Mobile session reports only have usage data for the Salesforce Mobile Classic app and not other Salesforce mobile apps, such as the Salesforce app.
- Some devices do not provide every physical attribute. For example, Apple devices do not provide brand.

Manage Salesforce Mobile Classic Devices

After a user installs the Salesforce Mobile Classic app on a mobile device and logs in for the first time, Salesforce collects information about the device and associates it with the user's record. The device information is read only.

Although the device entry is created automatically, you can still view and manage all the mobile users and devices in your organization from Setup by entering *Users and Devices* in the Quick Find box, then selecting **Users and Devices**.

From the All Mobile Users and Devices page, you can:

- View the list of users in your organization who have been enabled to use Salesforce Mobile Classic.
- Create custom list views to see different subsets of your mobile users. For example, create a view that shows the users who have never logged in to Salesforce from theSalesforce Mobile Classic app to evaluate the effectiveness of your organization's Salesforce Mobile Classic deployment efforts.
- View details about a mobile device by clicking the device address.
- View details about a specific user by clicking the username.
- View details about a mobile configuration by clicking the mobile configuration name.
- Perform these actions on multiple users at the same time:
  - Adjust the mobile session timeout value
  - Erase the Salesforce data from a user's mobile device
  - Delete a mobile device from a user's record
- Find out why a user's device isn’t synchronizing by hovering your mouse over the red error icon in the Status column. Additional information about the synchronization errors appears on the device's detail page.

Note: You can also manage mobile users from the Assigned Mobile Devices related list on the user detail page.

SEE ALSO:

Support On-the-Go Productivity with Salesforce Mobile Classic

Manage Salesforce Mobile Classic Configurations

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter ’17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter ’17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic devices and users:

- View Setup and Configuration

To manage Salesforce Mobile Classic devices:

- Manage Mobile Configurations

Permanently Link Salesforce Mobile Classic Users to a Mobile Device

You can prevent mobile users from registering any mobile device other than the one they used for their initial Salesforce Mobile Classic activation.

By default, Salesforce automatically associates a device record with the mobile user who most recently activated the device, so administrators don't need to update the device record to assign the device to another user. While this behavior makes it easy to switch devices between users in your organization, some administrators prefer that users are permanently linked to the devices they were originally assigned. This helps administrators of organizations with highly sensitive data ensure that their users do not access corporate data from personal devices.

To permanently link a user to a mobile device:

1. From Setup, enter `Salesforce Classic Settings` in the `Quick Find` box, then select **Salesforce Classic Settings**.
2. Click **Edit**.
3. Select `Permanently Link User to Mobile Device`.
4. Click **Save**.

Warning: Enabling the `Permanently Link User to Mobile Device` setting requires administrative action when users need to switch devices. You must manually delete the existing device from a user's record in order for the user to register a different device. If you don't delete the device, the user won't be able to access the Salesforce Mobile Classic app.

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic settings:

- View Setup and Configuration

To change Salesforce Mobile Classic settings:

- Manage Mobile Configurations

Viewing Salesforce Mobile Classic Device Information

Salesforce collects information about a mobile user's device the first time the user logs in to the Salesforce Mobile Classic app. There are two ways to access the device details.

- From Setup, enter `Users and Devices` in the `Quick Find` box, then select **Users and Devices**. Then click a device address in the list view.
- From Setup, enter `Users` in the `Quick Find` box, then select **Users**. Click **Edit** next to a user's name, and then click the device address in the Assigned Mobile Devices related list.

From the Mobile Device page, you can:

- Review device information
- Adjust the mobile session timeout value
- Erase the Salesforce data from a user's device
- Delete a device from a user's record

Below is a description of the fields in alphabetical order that are stored for each mobile device in your organization.

Field	Description
`Brand`	The brand of the mobile device, if available.
`Carrier`	The name of the carrier providing service for the mobile device, if available.
`Connected Since`	The date and time the device established a connection to the mobile server. The device loses a connection when the battery dies or when the session is closed because the server has not received data from the device for a long period of time.
`Connection Status`	The state of the device connection. Possible values for this field are Connected, Not Connected, and Not Available.
`Created By`	The name of the first user who registered the mobile device and the time and date the registration occurred.
`Data Size`	The size of the Salesforce data currently stored on the user's mobile device. The mobile device periodically sends this information to Salesforce, which is helpful when troubleshooting synchronization errors resulting from an exceeded data limit.
`Device Address`	The unique identifier of the user's mobile device.
`Device Model`	The model of the mobile device.
`Is Simulator?`	A flag indicating whether the device is a simulator or a mobile device. A simulator is a

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view Salesforce Mobile Classic devices and users:

- View Setup and Configuration

To manage Salesforce Mobile Classic devices:

- Manage Mobile Configurations

Field	Description
	software application that emulates the behavior of a mobile device.
`Last Activated`	The last time a full data set was downloaded to the mobile device. If a user's data set exceeds the limit defined in the assigned mobile configuration, the device can be registered but not activated.
`Last Data Received`	The last time data was received from the device. This information is helpful for troubleshooting connection issues.
`Last Registration`	The last time a user registered the mobile device. The registration process creates the device record in Salesforce and associates it with the user who registered it.
`Last Status Date`	The last time the mobile device notified Salesforce that the device is no longer synchronizing data due to an error. The `Last Status Date` field is only visible when an error is present.
`Manufacturer`	The manufacturer of the mobile device.
`Metadata Size`	The size of the Salesforce metadata currently stored on the user's mobile device. Metadata consists of page layout and schema information, and the amount of metadata sent to a device can be very high depending on the size of your organization and the complexity of its setup.
`Modified By`	The name of the last user who registered the mobile device and the time and date the registration occurred.
`Number of Pending Outgoing Messages`	The number of messages queued on the mobile server waiting to be sent to the device.
`Operating System`	The type of operating system installed on the mobile device: Android or iPhone.
`Operating System Version`	The version number of the operating system installed on the mobile device.
`Phone Number`	The phone number associated with the mobile device.
`Salesforce Mobile Classic Version`	The version number and build number of the mobile client application installed on the device.
`Size of Pending Outgoing Messages (Bytes)`	The total data size of the messages queued on the device waiting to be sent to the mobile server. Because the server processes messages almost instantaneously, this value is usually 0.
`Size of Outgoing Messages (Bytes)`	The total data size of the outbound message queue on the mobile server.
`Status`	Indicates whether any synchronization errors exist between the device and Salesforce. The `Status` field is only visible when an error is present. The two error statuses are Data Limit Exceeded and Unknown Error.

Field	Description
`Username`	The Salesforce username of the user who is associated with the mobile device.

Note: If Salesforce detects the selected device was registered by a user in another organization, an error displays on the device detail page. This can happen when a device was registered to a user in your sandbox organization and then later activated by a user in your production organization. To remove the old device record from your organization, simply delete the device.

Set Salesforce Mobile Classic Session Timeout Values

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To set Salesforce Mobile Classic session timeout values:

- Manage Mobile Configurations

For security reasons, the Salesforce Mobile Classic app is set to lock out users after 10 minutes of inactivity. Administrators can adjust or disable this setting on a device-by-device basis. For example, you might disable the Salesforce Mobile Classic timeout setting if a mobile device's operating system has its own locking mechanism.

To change the Salesforce Mobile Classic session timeout value:

1. Navigate to one of these pages.
   - To deal with multiple devices at the same time, from Setup, enter *`Users and Devices`* in the `Quick Find` box, then select **Users and Devices**. In the list view on the Mobile Users and Devices page, select the desired devices.
   - To deal with a specific device, from Setup, enter *`Users`* in the `Quick Find` box, then select **Users**. Click a user's name, then click the device address in the Assigned Mobile Devices related list to see the Mobile Device page.
2. Click **Set Mobile Session Timeout**.
3. Choose the new timeout value in minutes. You can also choose **Never Expire** if users shouldn't be locked out of the app.
4. Click **Save**.

   Salesforce attempts to send a message containing the new session timeout setting to the selected mobile devices.
5. A confirmation page summarizes the results for each mobile device you selected.

Mobile Session Timeout Results

After Salesforce sends the new session timeout session to the selected mobile devices, a results page provides information about the status of each message. The table below describes the three possible outcomes:

Result	Description
Message successfully queued	The Salesforce Mobile Classic server has sent the message to the device. Salesforce can't detect if the message was received by the device.
Unable to send message	A temporary communication problem between Salesforce and the Salesforce Mobile Classic

Result	Description
	server prevented the message from being sent. Try again later.
User has no mobile device	The selected mobile user never registered a device, so therefore the message could not be sent.

Erasing Data in Salesforce Mobile Classic

When a user accesses the Salesforce Mobile Classic app, the user's mobile device contains both the mobile app and a set of the user's Salesforce data. An administrator can remove the data from a device without uninstalling the mobile app. This is an effective security tool when a user misplaces his or her device. You also must erase a device's data if you plan to give it to another user.

To erase the Salesforce data on one or more mobile devices:

1. Navigate to one of these pages.
   - To deal with multiple devices at the same time, from Setup, enter `Users and Devices` in the `Quick Find` box, then select **Users and Devices**. In the list view on the Mobile Users and Devices page, select the desired devices.
   - To deal with a specific device, from Setup, enter `Users` in the `Quick Find` box, then select **Users**. Click a user's name, then click the device address in the Assigned Mobile Devices related list to see the Mobile Device page.
2. Click **Erase Data**, then click **OK**.

   Salesforce attempts to send a message to the mobile devices to erase the data.

Erase Data Results

After Salesforce sends the message to the mobile devices to erase data, a results page provides information about the status of each message. The table below describes the three possible outcomes:

Result	Description
Message successfully queued	The Salesforce Mobile Classic server has sent the message to the device. Salesforce can't detect if the message was received by the device.
Unable to send message	A temporary communication problem between Salesforce and the Salesforce Mobile Classic server prevented the message from being sent. Try again later.

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To delete the Salesforce data on a device running Salesforce Mobile Classic:

- Manage Mobile Configurations

Result	Description
User has no mobile device	The selected mobile user never registered a device, so therefore the message could not be sent.

SEE ALSO:

Manage Salesforce Mobile Classic Devices

Deleting Mobile Devices

Deleting Mobile Devices

There are two instances when you would delete a mobile device from a user's record:

- Your organization's mobile settings permanently link mobile users to their devices, and you need to assign a device to a different user. If you did not enable this setting, Salesforce automatically associates a device record with the mobile user who most recently activated the device, so it is unnecessary to delete a device to assign it to another user.
- You want to move a device from your sandbox organization to your production organization.

To delete a mobile device:

1. Navigate to one of these pages.
   - To deal with multiple devices at the same time, from Setup, enter *Users and Devices* in the Quick Find box, then select **Users and Devices**. In the list view on the Mobile Users and Devices page, select the desired devices.
   - To deal with a specific device, from Setup, enter *Users* in the Quick Find box, then select **Users**. Click a user's name, then click the device address in the Assigned Mobile Devices related list to see the Mobile Device page.
2. On the Mobile Devices and Users page, select one or more devices, then click **Delete Device**. On the Mobile Device page, click **Delete**.
3. Click **OK**.

   Salesforce attempts to delete the selected device(s).
4. A confirmation page summarizes the results for each mobile device you selected.

Delete Device Results

After Salesforce sends the message to the mobile server to delete the devices, a results page provides information about the status of each device. The table below describes the three possible outcomes:

Result	Description
Device deleted.	Salesforce removed the device record from your organization.
Device cannot be deleted at this time. Please try again later.	A temporary communication problem between Salesforce and the mobile server prevented the device from being deleted. Try again later.

EDITIONS

Salesforce Mobile Classic setup available in: both Salesforce Classic and Lightning Experience

Mobile app available in: **Performance**, **Unlimited**, and **Developer** Editions for orgs created prior to Winter '17

Mobile app available for an extra cost in: **Professional** and **Enterprise** Editions for orgs created prior to May 1, 2016

Mobile app not available for orgs created in Winter '17 or later

USER PERMISSIONS

To view mobile devices and users:

- View Setup and Configuration

To delete mobile devices:

- Manage Mobile Configurations

Result	Description
User has no mobile device.	The selected mobile user never registered a device, so therefore the message could not be sent.

SEE ALSO:

Erasing Data in Salesforce Mobile Classic

Salesforce Mobile Classic App Limits

Mobile Device Limits

Apple iPhone and iPod Touch devices	• Third parties (including, but not limited to, Apple Inc. and your network connectivity provider) may at any time restrict, interrupt or prevent use of Salesforce Mobile Classic for the iPhone and iPod touch devices, or delete the Salesforce Mobile Classic app from iPhone or iPod touch devices, or require Salesforce to do any of the foregoing, without entitling the customer to any refund, credit or other compensation from such third-party or Salesforce. • Service level agreements don't apply to the Salesforce Mobile Classic for iPhone product. Additional limitations are described in the Order Form Supplement for Salesforce Mobile Classic for iPhone, which users are required to accept upon download or installation of the Salesforce Mobile Classic for iPhone product.

Dashboards Limits

When working with dashboards in Salesforce Mobile Classic, these limitations exist:

- You can't create or edit dashboards.
- Links to custom report details are disabled.

View a Mobile User's Push Registration Information

With the Mobile Push Registrations Page, you can view any user's push registration information for general troubleshooting.

To view a user's device push registration information:

1. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.
2. Select a user.
3. On the user detail page next to `Mobile Push Registrations`, click **View**.

EDITIONS

Available in: Salesforce Classic

Available in: All editions

USER PERMISSIONS

To view mobile push registration information:

- View Setup and Configuration

Installed Packages

You can install packages into your Salesforce organization, and then configure and manage them. To view the packages you've installed, from Setup, enter "Installed" in the Quick Find box, and then select **Installed Packages**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Install a Package

Install a managed or unmanaged package in your Salesforce org to add new functionality to your org. Choose a custom installation to modify the default package settings, including limiting access to the package. Before you install a package, verify on the AppExchange listing that the offering is compatible with your Salesforce edition.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To install packages:

- Download AppExchange Packages

Pre-Installation Steps

1. In a browser, go to the installation URL provided by the package developer, or, if you're installing a package from the AppExchange, click **Get It Now** from the application information page.

   Note: If you're installing into a sandbox, replace the www.salesforce.com portion of the installation link with test.salesforce.com. The package is removed from your sandbox organization whenever you create a new sandbox copy.

2. Enter your username and password for the Salesforce organization in which you want to install the package, and then click the login button.
3. If the package is password-protected, enter the password you received from the publisher.

4. Optionally, if you're installing an unmanaged package, select **Rename conflicting components in package**. When you select this option, Salesforce changes the name of a component in the package if its name conflicts with an existing component name.

Default Installation

Click **Install**. You'll see a message that describes the progress and a confirmation message after the installation is complete.

Custom Installation

Follow these steps if you need to modify the default settings as an administrator.

1. Choose one or more of these options, as appropriate.
   - Click **View Components**. You'll see an overlay with a list of components in the package. For managed packages, the screen also contains a list of connected apps (trusted applications that are granted access to a user's Salesforce data after the user and the application are verified). Review the list to confirm that the components and any connected apps shown are acceptable, and then close the overlay.

     Note: Some package items, such as validation rules, record types, or custom settings might not appear in the Package Components list but are included in the package and installed with the other items. If there are no items in the Package Components list, the package might contain only minor changes.

   - If the package contains a remote site setting, you must approve access to websites outside of Salesforce. The dialog box lists all the websites that the package communicates with. We recommend that a website uses SSL (secure sockets layer) for transmitting data. After you verify that the websites are safe, select **Yes, grant access to these third-party websites** and click **Continue**, or click **Cancel** to cancel the installation of the package.

     Warning: By installing remote site settings, you're allowing the package to transmit data to and from a third-party website. Before using the package, contact the publisher to understand what data is transmitted and how it's used. If you have an internal security contact, ask the contact to review the application so that you understand its impact before use.

   - Click **API Access**. You'll see an overlay with a list of the API access settings that package components have been granted. Review the settings to verify they're acceptable, and then close the overlay to return to the installer screen.
   - In Enterprise, Performance, Unlimited, and Developer Editions, choose one of the following security options.

     Note: Depending on the type of installation, you might not see this option. For example, in Group and Professional Editions, or if the package doesn't contain a custom object, Salesforce skips this option, which gives all users full access.

     Install for Admins Only

     Specifies the following settings on the installing administrator's profile and any profile with the "Customize Application" permission.

     - Object permissions—"Read," "Create," "Edit," "Delete," "View All," and "Modify All" enabled
     - Field-level security—set to visible and editable for all fields
     - Apex classes—enabled
     - Visualforce pages—enabled
     - App settings—enabled
     - Tab settings—determined by the package creator
     - Page layout settings—determined by the package creator
     - Record Type settings—determined by the package creator

     After installation, if you have Enterprise, Performance, Unlimited, or Developer Edition, set the appropriate user and object permissions on custom profiles as needed.

Install for All Users

Specifies the following settings on all internal custom profiles.

- Object permissions—"Read," "Create," "Edit," and "Delete" enabled
- Field-level security—set to visible and editable for all fields
- Apex classes—enabled
- Visualforce pages—enabled
- App settings—enabled
- Tab settings—determined by the package creator
- Page layout settings—determined by the package creator
- Record Type settings—determined by the package creator

Note: The Customer Portal User, Customer Portal Manager, High Volume Customer Portal, Authenticated Website, Partner User, and standard profiles receive no access.

Install for Specific Profiles...

Enables you to choose the usage access for all custom profiles in your organization. You can set each profile to have full access or no access for the new package and all its components.

- Full Access—Specifies the following settings for each profile.
  - Object permissions—"Read," "Create," "Edit," "Delete," "View All," and "Modify All" enabled
  - Field-level security—set to visible and editable for all fields
  - Apex classes—enabled
  - Visualforce pages—enabled
  - App settings—enabled
  - Tab settings—determined by the package creator
  - Page layout settings—determined by the package creator
  - Record Type settings—determined by the package creator
- No Access—Specifies the same settings as Full Access, *except* all object permissions are disabled.

You might see other options if the publisher has included settings for custom profiles. You can incorporate the settings of the publisher's custom profiles into your profiles without affecting your settings. Choose the name of the profile settings in the drop-down list next to the profile that you need to apply them to. The current settings in that profile remain intact.

Alternatively, click **Set All** next to an access level to give this setting to all user profiles.

2. Click **Install**. You'll see a message that describes the progress and a confirmation message after the installation is complete.
   - During installation, Salesforce checks and verifies dependencies. An installer's organization must meet all dependency requirements listed on the Show Dependencies page or else the installation will fail. For example, the installer's organization must have divisions enabled to install a package that references divisions.
   - When you install a component that contains Apex, all unit tests for your organization are run, including the unit tests contained in the new package. If a unit test relies on a component that is initially installed as inactive, such as a workflow rule, this unit test might fail. You can select to install regardless of unit test failures.
   - If your installation fails, see Why did my installation or upgrade fail? on page 926.

Post-Installation Steps

If the package includes post-installation instructions, they're displayed after the installation is completed. Review and follow the instructions provided. In addition, before you deploy the package to your users, make any necessary changes for your implementation. Depending on the contents of the package, you might need to perform some of the following customization steps.

- If the package includes permission sets, assign the included permission sets to your users who need them. In managed packages, you can't make changes to permission sets that are included in the package, but subsequent upgrades happen automatically. If you clone a permission set that comes with a managed package or create your own, you can make changes to the permission set, but subsequent upgrades won't affect it.
- If you're re-installing a package and need to re-import the package data by using the export file that you received after uninstalling, see Importing Package Data on page 919.
- If you installed a managed package, click **Manage Licenses** to assign licenses to users.

  Note: You can't assign licenses in Lightning Experience. If you need to assign a license, switch to Salesforce Classic.
- Configure components in the package as required. For more information, see Configuring Installed Packages on page 911.

SEE ALSO:

Upgrading Packages

Installation Guide: Installing Apps from Force.com AppExchange

Installed Packages

Configuring Installed Packages

Many components have an **Is Deployed** attribute that controls whether they are available for end users. After installation, all components are immediately available if they were available in the developer's organization. Before making the package available to your users, make any necessary changes for your implementation. Depending on the contents of the package, you might need to customize the following items:

Configure Option

If the publisher included a link to an external website with information about configuration, AppExchange Downloads page displays a **Configure** option next to the package in Setup when you click **Installed Packages**. Click **Configure** to view the publisher's suggested configurations.

Custom Fields and Custom Links

Add any necessary custom fields or links to the new custom objects.

Custom Object

Enable tracking on objects that aren't in this package, but that have fields that are tracked in Chatter. For example, if you want to track a custom field on Account, you must make sure the Account standard object is enabled for tracking.

Custom Report Types

If the `Report Type Name` of a custom report type matches one used within your organization, change the `Report Type Name` after you install the package to avoid any confusion between the two report types.

Dashboard Running User

The `Running User` for any dashboards are set to the user installing the package. You can edit the properties of the dashboard and change the `Running User` to a user that has the security settings you want applied to the dashboard.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To install packages:
- Download AppExchange Packages

To configure installed packages:
- Customize Application

Folders

When apps contain documents, email templates, reports, or dashboards, Salesforce creates new folders in the installer's organization using the publisher's folder names. Make sure these folder names are unique in your organization.

All users can see new folders. Configure folder settings before you deploy if you want them to have limited visibility.

Home Page Layouts

Custom home page layouts included in the package are not assigned to any users. To make them available to your users, assign them to the appropriate profiles.

List Views

List views included in apps are visible to all users. Change the visibility of these list views if necessary.

Page Layouts

All users are assigned the default page layout for any custom objects included in the package. Administrators of Enterprise, Unlimited, Performance, and Developer Edition organizations can configure the page layout for the appropriate users.

If a custom object in the package includes any relationships to standard objects, add them as related lists on the appropriate page layouts.

If the package includes any custom links, add them to the appropriate page layouts.

If your organization has advanced currency management enabled, currency roll-up summary fields are invalid if they are on accounts and summarizing opportunity values, or on opportunities and summarizing custom object values. Remove these fields from any page layouts.

Permission Sets

Assign permission sets included in a package to the users who need access to the package.

You can't edit permission sets that are included in a managed package. If you clone a permission set that comes with the package or create your own, you can make changes to the permission set, but subsequent upgrades won't affect it.

Translation Workbench

Translated values for installed package components are also installed for any language that the developer has included. Any package components the developer has customized within setup, such as a custom field or record type, display in the installer's setup pages in the developer's language (the language used when defining these components). Users in the installer's organization automatically see translated values if their personal language is included in the package. Additionally, installers can activate additional languages as long as the Translation Workbench is enabled.

Workflow Alerts

If the recipient of a workflow alert is a user, Salesforce replaces that user with the user installing the package. You can change the recipients of any installed workflow alerts.

Workflow Field Updates

If a field update is designed to change a record owner field to a specific user, Salesforce replaces that user with the user installing the package. You can change the field value of any installed field updates.

Workflow Outbound Messages

Salesforce replaces the user in the `User to send as` field of an outbound message with the user installing the package. You can change this value after installation.

Workflow Rules

Workflow rules are installed without any time-based triggers that the developer might have created. Set up time-based triggers as necessary.

Workflow Tasks

Salesforce replaces the user in the `Assigned To` field with the user installing the package. You can change this value after installation.

Make any more customizations that are necessary for your implementation.

Note: Anything you add to a custom app after installation will be removed with the custom app if you ever uninstall it.

SEE ALSO:

Installed Packages

Tradeoffs and Limitations of Shield Platform Encryption

Uninstalling a Package

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To uninstall packages:

- Download AppExchange Packages

You can remove any installed package, including all its components and all data in the package. Also, any custom fields, links, or anything else you added to the custom app after installation are also removed.

To remove a package:

1. From Setup, enter `Installed` in the `Quick Find` box, then select **Installed Packages**.
2. Click **Uninstall** next to the package that you want to remove.
3. Select `Yes, I want to uninstall...` and click **Uninstall**.
4. After an uninstall, Salesforce automatically creates an export file containing the package data, associated notes, and any attachments. When the uninstall is complete, Salesforce sends an email containing a link to the export file to the user performing the uninstall. The export file and related notes and attachments are listed below the list of installed packages. We recommend storing the file elsewhere because it's only available for a limited time after the uninstall completes.

   Tip: If you reinstall the package later and want to reimport the package data, see Importing Package Data on page 919.

Notes on Uninstalling Packages

- If you're uninstalling a package that includes a custom object, all components on that custom object are also deleted. This includes custom fields, validation rules, s-controls, custom buttons and links, workflow rules, and approval processes.
- You can't uninstall a package whenever any component in the package is referenced by a component that will not get included in the uninstall. For example:
  - When an installed package includes any component on a standard object that another component references, Salesforce prevents you from uninstalling the package. This means that you can install a package that includes a custom user field and build a workflow rule that gets triggered when the value of that field is a specific value. Uninstalling the package would prevent your workflow from working.
  - When you have installed two unrelated packages that each include a custom object and one custom object component references a component in the other, Salesforce prevents you from uninstalling the package. This means that you can install an expense report app that includes a custom user field and create a validation rule on another installed custom object that references that custom user field. However, uninstalling the expense report app prevents the validation rule from working.
  - When an installed folder contains components you added after installation, Salesforce prevents you from uninstalling the package.
  - When an installed letterhead is used for an email template you added after installation, Salesforce prevents you from uninstalling the package.

- You can't uninstall a package if a field added by the package is being updated by a background job, such as an update to a roll-up summary field. Wait until the background job finishes, and try again.
- Uninstall export files contain custom app data for your package, excluding some components, such as documents and formula field values.
- For some package types, you can also uninstall them with the Salesforce command-line interface (CLI).

Manage Installed Packages

Manage packages installed in your Salesforce org, including assigning licenses to users, uninstalling packages, and exporting package data.

Note: Salesforce only lists license information for managed packages. For unmanaged packages, the license-related fields, such as **Allowed Licenses**, **Used Licenses**, and **Expiration Date**, displays the value "N/A."

Using this list, you can:

- Click **Uninstall** to remove the package and all its components from your Salesforce organization.
- Click **Manage Licenses** to assign available licenses to users in your organization. You can't assign licenses in Lightning Experience. If you need to assign a license, switch to Salesforce Classic.

  Note: If you purchased a site license or if the managed package is not licensed, Salesforce assigns licenses to all your users and you can't manage licenses. Your users can use the package as long as they have the appropriate permissions.

- Click **Configure** if the publisher has included a link to an external website with information about configuring the package.
- Click the package name to view details about this package.
- View the publisher of the package.
- View the status of the licenses for this package. Available values include:
  - Trial
  - Active
  - Suspended
  - Expired
  - Free

  This field is only displayed if the package is managed and licensed.

- Track the number of licenses available (`Allowed Licenses`) and the number of licenses that are assigned to users (`Used Licenses`).
- View the date your licenses for this package are scheduled to expire.
- View the date your licenses were installed.
- View the number of custom apps, tabs, and objects this package contains.
- See whether the custom apps, tabs, and objects count toward your organization's limits. If they do, the box in the `Limits` column is checked.

Note: If you have not installed a licensed managed package, the `Publisher`, `Status`, `Allowed Licenses`, `Used Licenses`, and `Expiration Date` fields do not appear.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To uninstall packages:
- Download AppExchange Packages

To assign licenses for a managed package:
- Manage Package Licenses

To download or delete the export file for an uninstalled package:
- Download AppExchange Packages

After an uninstall, Salesforce automatically creates an export file containing the package data, associated notes, and any attachments. When the uninstall is complete, Salesforce sends an email containing a link to the export file to the user performing the uninstall. The export file and related notes and attachments are listed below the list of installed packages. We recommend storing the file elsewhere because it's only available for a limited time after the uninstall completes. Using this list, you can:

- Click **Download** to open or store the export file.
- Click **Del** to delete the export file.

Expired Managed Packages and Sharing Rules

If a criteria-based sharing rule references a field from a licensed managed package whose license has expired, `(expired)` is appended to the label of the field. The field label is displayed in the field drop-down list on the rule's definition page in Setup. Criteria-based sharing rules that reference expired fields aren't recalculated, and new records aren't shared based on those rules. However, the sharing of existing records prior to the package's expiration is preserved.

SEE ALSO:

View Installed Package Details

Importing Package Data

View Installed Package Details

View key details about a package installed from the AppExchange, such as the number of custom apps, tabs, and objects it uses. You can also assign licenses to users, uninstall the package, and purchase the package.

To access the package detail page, from Setup, enter *`Installed Packages`* in the `Quick Find` box, select **Installed Packages**, and then click the name of the package that you want to view.

From this page, you can:

- Click **Uninstall** to remove the package and all its components from your Salesforce organization.
- Click **Manage Licenses** to assign available licenses to users in your organization. You can't assign licenses in Lightning Experience. If you need to assign a license, switch to Salesforce Classic.

  Note: If you purchased a site license or if the managed package is not licensed, Salesforce assigns licenses to all your users and you can't manage licenses. Your users can use the package as long as they have the appropriate permissions.

- Optionally, click **View Dependencies** and review a list of components that rely on other components, permissions, or preferences within the package.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To uninstall packages:

- Download AppExchange Packages

To manage user licenses for an AppExchange package:

- Manage Package Licenses

Viewing Installed Packages

The installed package page lists the following package attributes (in alphabetical order):

Attribute	Description
`Action`	Can be one of two options: - **Uninstall** - **Manage Licenses**

Attribute	Description
`Allowed Licenses`	The total number of licenses you purchased for this package. The value is “Unlimited” if you have a site license for this package. This field is only displayed if the package is managed and licensed.
`Apps`	The number of custom apps in the package.
`Connected Apps`	A list of the connected apps that can have access to a user's Salesforce data after the user and the application have been verified.
`Description`	A detailed description of the package.
`Expiration Date`	The date that this license expires, based on your terms and conditions. The expiration date is “Does Not Expire” if the package never expires.This field is only displayed if the package is managed and licensed.
`Installed Date`	The date of the package installation.
`Limits`	If checked, the package’s custom apps, tabs, and objects count toward your organization’s limits.
`Namespace`	The 1- to 15-character alphanumeric identifier that distinguishes a package and its contents from packages of other developers on AppExchange.
`Objects`	The number of custom objects in the package.
`Package Name`	The name of the package, given by the publisher.
`Publisher`	The publisher of an AppExchange listing is the Salesforce user or organization that published the listing. This field is only displayed if the package is managed and licensed.
`Status`	The state of a package. Available values include: • Trial • Active • Suspended • Expired • Free This field is only displayed if the package is managed and licensed.
`Tabs`	The number of custom tabs in the package.
`Used Licenses`	The total number of licenses that are already assigned to users. This field is only displayed if the package is managed and licensed.
`Version Name`	The version name for this package version. The version name is the marketing name for a specific release of a package. It is more descriptive than the `Version Number`.

Viewing Installed Package Details

The installed package detail page lists the following package attributes (in alphabetical order):

Attribute	Description
`Apps`	The number of custom apps in the package.
`Description`	A detailed description of the package.
`First Installed Version Number`	The first installed version of the package in your organization. This field is only displayed for managed packages. You can reference this version and any subsequent package versions that you have installed. If you ever report an issue with a managed package, include the version number in this field when communicating with the publisher.
`Installed By`	The name of the user that installed this package in your organization.
`Limits`	If checked, the package's custom apps, tabs, and objects count toward your organization's limits.
`Modified By`	The name of the last user to modify this package, including the date and time.
`Namespace`	The 1- to 15-character alphanumeric identifier that distinguishes a package and its contents from packages of other developers on AppExchange.
`Objects`	The number of custom objects in the package.
`Package Name`	The name of the package, given by the publisher.
`Package Type`	Indicates whether the package is managed or unmanaged.
`Post Install Instructions`	A link to information on configuring the package after it's installed. As a best practice, the link points to an external URL, so you can update the information independently of the package.
`Publisher`	The publisher of an AppExchange listing is the Salesforce user or organization that published the listing. This field is only displayed if the package is managed and licensed.
`Release Notes`	A link to release notes for the package. As a best practice, link to an external URL, so you can make the information available before the release and update it independently of the package.
`Tabs`	The number of custom tabs in the package.
`Version Name`	The version name for this package version. The version name is the marketing name for a specific release of a package. It is more descriptive than the `Version Number`.
`Version Number`	The version number for the latest installed package version. The format is *`majorNumber.minorNumber.patchNumber`*,

Attribute	Description
	such as 2.1.3. The version number represents a release of a package. The `Version Name` is a more descriptive name for the release. The `patchNumber` is generated only when you create a patch. If there is no `patchNumber`, it is assumed to be zero (0).

Unused Components

You can see a list of components deleted by the developer in the current version of the package. If this field is part of a managed package, it's no longer in use and is safe to delete unless you've used it in custom integrations. Before deleting a custom field, you can keep a record of the data from Setup by entering *`Data Export`* in the `Quick Find` box, then selecting **Data Export**. After you've deleted an unused component, it appears in this list for 15 days. During that time, you can either undelete it to restore the field and all data stored in it, or delete the field permanently. When you undelete a field, some properties on the field are lost or changed. After 15 days, the field and its data are permanently deleted.

The following component information is displayed (in alphabetical order):

Attribute	Description
`Action`	Can be one of two options: • **Undelete** • **Delete**
`Name`	Displays the name of the component.
`Parent Object`	Displays the name of the parent object a component is associated with. For example, a custom object is the parent of a custom field.
`Type`	Displays the type of the component.

Package Components

You can see a list of the components included in the installed package. The following component information is displayed (in alphabetical order):

Attribute	Description
`Action`	Can be one of two options: • **Undelete** • **Delete**
`Name`	Displays the name of the component.
`Parent Object`	Displays the name of the parent object a component is associated with. For example, a custom object is the parent of a custom field.

Attribute	Description
`Type`	Displays the type of the component.

SEE ALSO:

Importing Package Data

Manage Installed Packages

Importing Package Data

When you uninstall an AppExchange package, Salesforce automatically creates an export file containing the package data as well as any associated notes and attachments. If you choose to install the package again, you can import this data.

To import your AppExchange package data, use one of the following tools that is available for your Edition:

- For Group Edition, use the appropriate import wizard.
- For Professional Edition, use the appropriate import wizard or any compatible Salesforce ISV Partner integration tool.
- For Enterprise, Developer, Performance, and Unlimited Edition, use the Data Loader.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To import Force.com AppExchange package data:

- The permissions required to use the import tool you choose, such as the import wizard or Data Loader.

Notes on Importing AppExchange Package Data

- Salesforce converts date fields into date/time fields upon export. Convert the appropriate fields into date fields before you import.
- Salesforce exports all date/time fields in Greenwich Mean Time (GMT). Before importing these fields, convert them to the appropriate time zone.
- The value of auto number fields may be different when you import. To retain the old values, create a new custom auto number field on a custom object before importing the data.
- Salesforce updates system fields such as `Created Date` and `Last Modified Date` when you import. To retain the old values for these fields, contact Salesforce support.
- Relationships are not included in the export file. Recreate any master-detail or lookup relationships after importing your data.
- Record type IDs are exported but not the record type name.
- Field history is not exported.
- Recreate any customizations that you made to the package after installation.

SEE ALSO:

View Installed Package Details

Manage Installed Packages

Managing Licenses for Installed Packages

When you install a licensed managed package in your organization from AppExchange, you purchase a certain number of licenses from the package developer or publisher. You can assign each license to a user within your organization. If you assign all available licenses, but would like to grant licenses to additional users, you can reassign a license or purchase more. To get more licenses, contact the publisher of the managed package.

Note: If you purchased a site license or if the managed package is not licensed, Salesforce assigns licenses to all your users and you can’t manage licenses. Your users can use the package as long as they have the appropriate permissions.

1. From Setup, enter `Installed Packages` in the `Quick Find` box, then select **Installed Packages**.
2. Click **Manage Licenses** next to the package.

   Note: To assign licenses for a package, you must have access to the package and at least one available license.

   - To assign licenses to more users, click **Add Users**.
   - To remove a license from a user, click **Remove** next to the user's name. To remove licenses from multiple users, click **Remove Multiple Users**.
   - Click any column heading to sort the users in ascending order using the data in that column. Click the heading again to sort in descending order.
   - If available, select **fewer** or **more** to view a shorter or longer display list.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To manage licenses for a AppExchange package:

- Manage Package Licenses

SEE ALSO:

Assign Licenses for Managed Packages

Assigning Licenses for Installed Packages

Removing Licenses for Installed Packages

Responding to License Manager Requests

Assign Licenses for Managed Packages

When you install a licensed managed package in your organization from AppExchange, you purchase a certain number of licenses from the package developer or publisher. You can assign each license to a user within your organization. If you assign all available licenses, but would like to grant licenses to additional users, you can reassign a license or purchase more. To get more licenses, contact the publisher of the managed package.

The Managed Packages related list on the user detail page lists all managed packages that user is assigned. Assigning a license for a managed package makes the package available to the user within Salesforce. Unmanaged packages don't appear on this list because you can't assign licenses for them.

Note: If you purchased a site license or if the managed package is not licensed, Salesforce assigns licenses to all your users and you can't manage licenses. Your users can use the package as long as they have the appropriate permissions.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To edit users:
- Manage Internal Users

To manage licenses for an AppExchange package:
- Manage Package Licenses

To assign a user to a license for one of the available managed packages:

1. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.
2. Click **Assign Licenses** from the Managed Packages list.
3. Select the package you want to assign to the user. All available managed packages are listed in the Unassigned Packages list. After selecting a package, Salesforce automatically moves it to the Selected Packages list.

   The Unassigned Packages list displays all packages that this user could access if assigned a license. Packages don't appear on this list if they are unmanaged, uninstalled, in use, or not available.

   - Click a letter to view the packages that begin with that letter or click **All** to display all available managed packages.
   - Click **select shown** to select all packages displayed in the Unassigned Packages list on the current page, adding them to the Selected Packages list below.
   - Click **deselect shown** or **deselect all** to move packages from the Selected Packages area to the Unassigned Packages area.

4. Click **Add**.

To revoke a license from this user, click the **Remove** link next to the appropriate package name.

SEE ALSO:

Managing Licenses for Installed Packages

Assigning Licenses for Installed Packages

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To manage licenses for an AppExchange app:

- Manage Package Licenses

To assign licenses to Force.com AppExchange users:

Note: If you purchased a site license or if the managed package is not licensed, Salesforce assigns licenses to all your users and you can't manage licenses. Your users can use the package as long as they have the appropriate permissions.

1. From Setup, enter `Installed Packages` in the `Quick Find` box, then select **Installed Packages** to find the installed package that has available licenses.
2. Click the **Manage Licenses** link next to the package name.
3. Click **Add Users**.
4. Choose a view from the drop-down list, or click **Create New View** to build a new custom view.
5. Click a letter to filter the users with a last name that corresponds with that letter or click **All** to display all users who match the criteria of the current view.
6. Select users.
   - To select individual users, use the checkboxes. Selected users are listed in the Selected list. When the list includes all users to which you want to assign licenses, click **Add**.
   - To select all users for the current view, click **Add All Users** then click **OK**.

Note: You can also add a single user from the user's detail page.

SEE ALSO:

Managing Licenses for Installed Packages

Removing Licenses for Installed Packages

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To manage licenses for an AppExchange package:

- Manage Package Licenses

To remove licenses for an AppExchange package from multiple users:

1. From Setup, enter `Installed Packages` in the `Quick Find` box, then select **Installed Packages**.
2. Click **Manage Licenses** next to the package name.
3. Click **Remove Multiple Users**.
4. To show a filtered list of items, select a predefined list from the `View` drop-down list, or click **Create New View** to define your own custom views.
5. Click a letter to filter the users with a last name that corresponds with that letter or click **All** to display all users who match the criteria of the current view.
6. Select users.
   - To select individual users, use the checkboxes. Selected users appear in the Selected for Removal list. When the list includes all users for which you want to remove licenses, click **Remove**.
   - To select all users in the current view, click **Remove All Users**, then click **OK**.

You can also remove licenses for an AppExchange package from a single user using the following options:

1. From Setup, enter `Users` in the `Quick Find` box, then select **Users** and click **Remove** next to the package in the managed packages list.

2. From Setup, enter `Installed Packages` in the `Quick Find` box, then select **Installed Packages**. Then, click **Manage Licenses** next to the package name, and click **Remove** next to the user.

SEE ALSO:

Managing Licenses for Installed Packages

Responding to License Manager Requests

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Developer** Edition

Package uploads and installs are available in **Group**, **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To respond to registration requests:

- Customize Application

A license manager is a Salesforce organization that tracks all Salesforce subscribers installing a particular AppExchange package. Salesforce administrators can choose to designate another organization as the license manager for one of their packages. The license manager does not need to be the same organization as the one from which the package is managed. To choose another organization as the license manager, all you need is an email address (not a Salesforce username). If a Salesforce administrator selects to have a third-party license manager and enters your email address, you will receive a license management request in email.

To respond to a registration request:

1. Click the link in the license management request email. This displays the registration request in the requestor's Developer Edition organization.
2. Click **Accept** to complete the registration process. Alternatively, click **Reject** to decline the request and close the browser; this prevents you from using the link again.

   Note: If you accept this request, you authorize Salesforce to automatically create records in your Salesforce organization to track information about this package. Choosing a license manager organization is permanent and cannot be changed.

3. Enter the username and password for the Salesforce organization you want to use to manage licenses for this package. A license manager can be any Salesforce organization that has installed the free License Management Application (LMA) from Force.com AppExchange.
4. Click **Confirm**.

SEE ALSO:

Managing Licenses for Installed Packages

Assigning Licenses Using the API

Administrators can use the API to assign or revoke licenses for any managed package installed in their organization. License information for a package is stored in two objects, PackageLicense and UserPackageLicense, which were previously accessible only from the Manage Licenses page under Setup. These are now accessible as standard objects, so an administrator can assign licenses to specific users via API calls. This makes managing package licenses in a subscriber organization faster and easier, especially for large-scale deployments.

For example, suppose an administrator installs an app for use by all 200 salespeople in the company. Assigning a license to each salesperson from the UI is inefficient and time-consuming. Using the API, the administrator can assign licenses to all salespeople, based on their profile, in one step.

Here are some common licensing tasks that administrators can use the API to do.

- Determine the number of package licenses in use and available.
- Verify if a specific user has a license for the package.
- Get a list of all users who have a license for the package.
- Assign a package license to a user or group of users.
- Revoke a package license that was previously assigned to a user.

For details of the PackageLicense and UserPackageLicense objects and a code sample, see the Object Reference for Salesforce and Force.com.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To manage licenses for an AppExchange app:

- Manage Package Licenses

Upgrading Packages

Salesforce supports upgrades for managed packages only. Publishers can publish an upgrade for a managed package and notify installers that the new version is available. Installers of a managed package can then install the upgrade as follows:

1. Before you install an upgrade, determine if the app you installed was from a managed package. Look for the Managed - Installed icon on the detail pages for each component and on the list of packages installed.

   If the app you installed is not from a managed package, upgrades for it are not available.

2. Then, install the upgrade in the same way you would install any other package from the AppExchange. If the publisher provided a link to the new version, follow the link to the package posting and install it in your organization. The first page of the install wizard lists the current version you have installed, the version you're about to install, and a list of additional components included in the new version.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To upload packages:

- Upload AppExchange Packages

To install and uninstall packages:

- Download AppExchange Packages

Notes on Upgrading Managed Packages

Consider the following when upgrading a managed package:

- All existing custom objects that were previously deployed will still be deployed. Salesforce prompts you to deploy any new custom objects or previously undeployed custom objects.
- Profile settings for components in a package are editable by the customer but not upgradeable by the package developer. If the developer makes changes to any profile settings after releasing the package, those changes won't be included in an upgrade. Customers will need to manually update the profile settings after upgrading the package. In contrast, permission sets in a package are upgradeable by the developer, so any changes the developer makes will be reflected in the customer organization after upgrading the package.

- If the developer chooses to add universally required custom fields, the fields will have default values.
- Translation Workbench values for components that are “editable but not upgradeable” are excluded from upgrades.
- If an installed package has `Restricted` API access, upgrades will be successful only if the upgraded version does not contain any s-controls. If s-controls are present in the upgraded version, you must change the currently installed package to `Unrestricted` API access.
- When you upgrade a package, changes to the API access are ignored even if the developer specified them. This ensures that the administrator installing the upgrade has full control. Installers should carefully examine the changes in package access in each upgrade during installation and note all acceptable changes. Then, because those changes are ignored, the administrator should manually apply any acceptable changes after installing an upgrade.

SEE ALSO:

Force.com Quick Reference for Developing Packages

Installing Packages FAQ

- Can I uninstall packages that I installed from AppExchange?
- Who can use AppExchange?
- Why did my installation or upgrade fail?
- Can I customize AppExchange packages?
- Who can use AppExchange packages?
- How can I upgrade an installed package?
- How secure are the components I install?
- What happens to my namespace prefix when I install a package?
- Can I reinstall an AppExchange package after uninstalling it?
- When I install a package that’s listed on the AppExchange, do custom objects, tabs, and apps in that package count against the limits of my Salesforce Edition?

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Can I uninstall packages that I installed from AppExchange?

Yes. All your installed packages are listed in the Installed Packages page. You can remove any package by clicking the **Uninstall** link next to the package name.

SEE ALSO:

Uninstalling a Package

Importing Package Data

Who can use AppExchange?

Anyone can browse and test drive AppExchange listings. Salesforce administrators and users with the “Download AppExchange packages” permission can install AppExchange apps. To publish an app on the AppExchange, a user must have both “Create AppExchange packages” and “Upload AppExchange packages” permissions.

Why did my installation or upgrade fail?

An installation can fail for several reasons:

- The package includes custom objects that will cause your organization to exceed its limit of custom objects.
- The package includes custom tabs that will cause your organization to exceed its limit of custom tabs.
- The developer of the package has uploaded a more recent version of the package and has deprecated the version associated with this installation URL. Contact the publisher of the package to get the most recent installation URL.
- You're trying to install an extension to a package, and you don't have the base package installed.
- The package requires that certain components are enabled in your organization, or that required features are enabled in your edition.
- The package contains Apex code and you are not authorized to run Apex in your organization.
- The package you're installing has a failing Apex test.

Can I customize AppExchange packages?

Yes, all packages are customizable. However, to ensure compatibility with future versions, some aspects of managed packages can't be changed.

For a list of components that are editable in a managed package, see ISVforce Guide.

Who can use AppExchange packages?

If you use an Enterprise, Unlimited, Performance, or Developer Edition organization, you can choose which user profiles have access to the package as part of the installation process. Packages installed in Professional and Group Edition organizations are installed with "Full Access" to all user profiles. However, regardless of Edition, all custom objects are installed in "In Development" mode which hides them from all standard users. Users must have the "Customize Application" permission to view custom objects in "In Development" mode. When you are ready to roll out the package to other users, change the custom object status to "Deployed."

How can I upgrade an installed package?

Managed packages are completely upgradeable. Before installing a package, contact the publisher to determine if it's managed.

How secure are the components I install?

Salesforce performs periodic security reviews of all publicly listed applications on AppExchange. When installing third party applications with access to data, these applications may have access to other data within the organization where the package was installed. Private listings do not go through a security review and administrators should inspect the application carefully before determining whether it should be installed within their organization.

What happens to my namespace prefix when I install a package?

A namespace prefix is a globally unique identifier that you can request if you plan to create a managed package. All the components from a managed package that you install from another developer contain the developer's namespace prefix in your organization. Unmanaged packages can have a namespace prefix while they're developed in an org that contains a managed package. This namespace isn't used outside of the development (publisher) org. If an unmanaged package is installed in an org that has no namespace, then the unmanaged components have no namespace in the subscriber org. If an unmanaged package is installed in an org that has a namespace, then the components get the namespace of the subscriber org.

Can I reinstall an AppExchange package after uninstalling it?

Yes. You can reinstall a package in the same manner that you installed it.

SEE ALSO:

Install a Package

Importing Package Data

When I install a package that's listed on the AppExchange, do custom objects, tabs, and apps in that package count against the limits of my Salesforce Edition?

No. If you install a package from the AppExchange, its custom objects, tabs, and apps don't count against the limits of your Salesforce edition. However, if the package uses other types of custom components, such as custom fields, they count against the relevant limits of your Salesforce edition.

Note: These rules apply only to managed packages that are listed on the AppExchange. If you install an unmanaged package or a managed package that's not publicly listed on the AppExchange, its custom objects, tabs, and apps count against the limits of your Salesforce edition.

Learn More About Setting Up Salesforce

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

Data Import

Guides and Tip Sheets	For End Users	For Admins
Data Loader Guide		✓
Importing Your Organization's Accounts and Contacts		✓
Using Mass Delete to Undo Imports		✓

Data Management

Guides and Tip Sheets	For End Users	For Admins
Salesforce Field Reference Guide	✓	
Getting Started with Divisions	✓	
Getting Started with Divisions	✓	
Resolving Data Conflicts and Errors in Force.com Flex Apps	✓	
Managing Duplicate Records in Salesforce		✓

Security

Guides and Tip Sheets	For End Users	For Admins
Security Implementation Guide		✓
Identity Connect Implementation Guide		✓
Platform Encryption Implementation Guide		✓
Salesforce Identity Implementation Guide		✓
Single Sign-On Implementation Guide		✓
Understanding User Sharing	✓	
Understanding Defer Sharing Calculations	✓	

INDEX