Set Up and Maintain Your Salesforce Organization

Salesforce, Spring '16

@salesforcedocs

Last updated: February 18, 2016

CONTENTS

SET UP AND MAINTAIN YOUR SALESFORCE ORGANIZATION

Welcome, Salesforce Administrators

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.

This guide contains the details you need to set up and maintain a Salesforce organization.

We hope this guide provides the complete content you need to get your organization up and running with Salesforce. If you need further support, contact the Support team at Salesforce.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: All Editions

Salesforce Trials

Trial Overview

During your trial, you can evaluate Salesforce before you subscribe. Your trial includes:

- Sample data. You can delete sample data or start a new trial.
- Administrator privileges. The person who signed up automatically becomes the administrator. You can add another administrator when you add more users.
- A variety of Salesforce features.
- The ability to subscribe to Salesforce.

Note: Features included in your trial may not be available in the Edition you choose to purchase.

If you set up multiple users in your trial and later choose to convert to Personal Edition, all users except the original system administrator will be deactivated.

EDITIONS

Available in: Salesforce Classic

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

Starting 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, you must abandon your current trial, including all data and customizations.

You can start a new trial if you have:

- Less than 1000 rows of data
- No additional user licenses added by Salesforce
- No additional functionality enabled by Salesforce

To start a new trial:

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 organization and all of its data. This includes both sample data and data you have entered.
4. Check the box to confirm that all of your current trial data will be lost.
5. Click **Submit**.
6. When the confirmation page appears, click **Submit**.

Note: By choosing to start a new trial, you are abandoning your current trial organization including all existing data and customizations. You will no longer be able to access the trial or data. Only usernames will be preserved.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

User Permissions Needed

To start a new trial:
- "Modify All Data"

Converting a Trial Using Checkout

Users with a Checkout account can convert a Salesforce trial into an Edition subscription. If your organization doesn't have self-service access to Checkout, submit a request to your Salesforce representative.

To convert your trial Edition into a subscription using Checkout, you must create a quote.

Note: At any point during the quote creation process, you can click **Request Assistance** to contact your Salesforce account representative.

To convert your trial Edition into a subscription:

1. To create a quote, click **Subscribe Now** or select Checkout from the Force.com Apps drop-down list. Note that the Edition and products used in your trial organization are preselected in Checkout.

   Important: If at any point during quote creation you close the window, you lose all changes. If you are creating a new quote, you lose the entire quote. You can click **Save for Later** on any page if you want to save your changes and continue editing it later.

2. If you are a new user, or creating or editing a quote from a trial, enter and confirm the information on the Subscription Information tab.
3. If you are creating or editing a quote from a trial of a larger Edition, enter and confirm the information on the Products page, review your billing information, and click **Jump to Order Review**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

4. If you want to create a quote for another Edition, click **Editions and Pricing**. Enter and confirm the subscription, product, and billing information, then click **Jump to Order Review**. The Order Review page displays the information you entered, as well as complete pricing for all products on the quote.

   Note: If you convert a trial organization to a lesser Edition, such as moving from a Professional Edition trial to a Group Edition subscription, some features and data from your trial are deleted. To accept the deletions, select the `Acknowledgment` checkbox. Click **Review this** to see a list of features not supported in your chosen Edition. If you want to back up all of your data before converting, log into your Salesforce organization and from Setup, enter *`Data Export`* in the `Quick Find` box, then select **Data Export**.

5. Verify your purchase and click **Place Order**.

As a trial user, if you create a quote and don't follow through with placing an order, the quote is saved in Checkout. Once you complete a quote and place an order for an Edition subscription, any other Edition quotes you have open are closed.

SEE ALSO:

Checkout User Guide

Delete Trial Data

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

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

- The user has the "Modify All Data" user permission.
- The organization is in a trial state.
- The organization 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 the data in your organization will be deleted. This includes both sample data and data you have entered. Your user and administration setup is not 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 Deleting Multiple Records and Reports on page 431.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To delete trial data:
- "Modify All Data"

Plan Your Salesforce Rollout

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

IN THIS SECTION:

How Can a Salesforce Consulting Partner Help Me?

Recently purchased Salesforce? Wondering how to get started? 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.
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	When consultants roll out Salesforce, there is a greater chance that sales teams adopt

Compare	Rolling out Salesforce Yourself	Rolling out Salesforce with a Partner
	don't recognize the products' value, and don't adopt the product wholeheartedly.	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 Organization

Find Company Information

Find the information that's provided when your company signed up with Salesforce on the Company Information page in Setup.

From the Company Information page, you can:

- Edit your company's information.
- View the user licenses, feature licenses, permission set licenses, and usage-based entitlements that your organization has access to.
- Add or remove licenses.
- (Sandbox organizations only) 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"

Company Information Fields

The Company Information page has the following fields (listed in alphabetical order), including the user and feature licenses purchased for your organization.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

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)
`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 will override 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

Field	Description
	stored. For customizations, individual users' language settings do not override this setting. If you edit or clone existing filter criteria, make sure this setting matches the default language that was configured when the filter criteria was originally set. Otherwise, the filter criteria may not be evaluated as 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 should select "Mountain Standard Time," and organizations in parts of Indiana that do not follow Daylight Savings Time should 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 will be "Custom Fiscal Year."
`Hide Notices About System Downtime`	Select this checkbox to prevent advance notices about planned system downtime from displaying to users when they log in to Salesforce.
`Hide Notices About System Maintenance`	Select this checkbox to prevent advance notices about planned system maintenance from displaying to users when they log in to Salesforce.
`Modified By`	User who last changed the company information, including modification date and time. (Read only)
`Newsletter`	Allow users in your organization to choose whether they want to receive user-targeted promotional emails from Salesforce.
`Organization Edition`	Edition of the organization, such as Developer Edition or Enterprise Edition.
`Organization Name`	Name of the organization. Up to 80 characters are allowed in this field.

Field	Description
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 is the number of 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%).
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:

Find Company Information

Required Domains

Salesforce uses these domains to deliver content.

- *.content.force.com
- *.force.com
- *.salesforce.com
- *.staticforce.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
- <instance>.salesforce.com (for example, na1.salesforce.com)
- A My Domain URL without custom branding (for example, norns.my.salesforce.com)

If you whitelist domains, add these 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.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: All Editions.

The Setup Menu

Improved Setup User Interface in Salesforce Classic

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

When the improved Setup user interface is enabled in an organization, you might notice 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.

EDITIONS

Available in: Salesforce Classic

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

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

Searching Setup with Advanced Setup Search (Beta)

With Advanced Setup Search, users can search for many types of items in Setup, 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, be sure 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 only the titles of pages in the Setup menu, not individual items that you might have 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'll immediately see Setup pages whose names match what you're typing. Click the name of the page to open it.
- To find Setup metadata, 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'll 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.

SEE ALSO:

Setup Search Results Page (Beta)

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:

Searching Setup with Advanced Setup Search (Beta)

Understanding Language, Locale, and Currency

The Salesforce settings for language, locale, time zone, and currency can affect how objects (Accounts, Leads, Opportunities, etc.) are displayed. In a single currency organization, the Salesforce administrators set the currency locale, default language, default locale, and default time zone for their organizations and the users can set their individual language, locale, and time zone on their personal settings pages. In a multiple currency organization, the Salesforce administrators set the corporate currency, default language, default locale, and default time zone for their organizations and the users can set their individual currency, language, locale, and time zone on their personal settings pages.

EDITIONS

Available in: Salesforce Classic

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

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

Setting	Who can edit the setting
Default Language	Administrator
Default Locale	Administrator
Default Time Zone	Administrator
Information Currency	Not editable
Language	User
Locale	User
Time Zone	User

SEE ALSO:

- Language Settings Overview
- Supported Currencies
- Which Languages Does Salesforce Support?
- Supported Locales
- Supported Time Zones
- Set Your Personal or Organization-Wide Currency

Language Settings Overview

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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

SEE ALSO:

- Understanding Language, Locale, and Currency

Which Languages Does Salesforce Support?

Salesforce offers three levels of language support: fully supported languages, end-user languages, and platform-only languages. Each language is identified by a two-character language code, 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 organizations in two ways. The Translation Workbench lets you specify languages you want to translate, assign translators to languages, create translations for customizations you've made to your Salesforce organization, and override labels and translations from managed packages. Everything from custom picklist values to custom fields can be translated so your global users can use all of 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 Setup by entering *Company Information* in the Quick Find box, selecting **Company Information**, then selecting **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 (Portugal): `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 Salesforce1 mobile 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

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:

- English (Australia), English (India), English (Malaysia), and English (Philippines) fall back to English (UK).
- German (Austria) and German (Switzerland) fall back to German.
- French (Canada) falls back to French.
- Romanian (Moldova) falls back to Romanian.
- Montenegrin falls back to Serbian (Latin).
- Portuguese (Portugal) 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`
- Chinese (Simplified—Singapore): `zh_SG`
- Chinese (Traditional—Hong Kong): `zh_HK`
- 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 (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:

Understanding Language, Locale, and Currency

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

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
							City, State ZipCode 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

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
Arabic (Morocco)	ar_MA	Moroccan Dirham: MAD	/ / : PM	:		Ms. FName LName	Address Line 1, Address Line 2 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

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							Country
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	02/28/2008 16:30	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

Name	Code	Default currency	Date and time format	Time format	Number format	Name format	Address format
							City, State ZipCode 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	2008-2-28 16:30	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	2008 2 28 PM4:30	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	2008 2 28 PM4:30	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	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 (Antigua and Barbuda)	en_AG	East Caribbean Dollar: XCD	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 (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	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 (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	2008-02-28 16:30	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	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
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	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
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:

Understanding Language, Locale, and Currency

Supported Time Zones

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)

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.

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:

Understanding 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: **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, users can set a personal currency that's different from their organization's corporate currency.

SEE ALSO:

Understanding 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.

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

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view currencies:
- "View Setup and Configuration"

To change currencies:
- "Customize Application"

Set Your Corporate Currency

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

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

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

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **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, users can set a personal currency that's different from their organization's corporate currency.

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

EDITIONS

Available in: 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.

SEE ALSO:

Set Your Personal or Organization-Wide Currency

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"

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

Fiscal Years

Define a fiscal year that fits your business needs.

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

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

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

Standard Fiscal Years

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

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"

Custom Fiscal Years

For companies that 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, as part of a custom fiscal year, you can create a 13-week quarter represented by three periods of 4, 4, and 5 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 by specifying a start date and choosing 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 that you need to change their definition. For example, an extra week could be added 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 cannot disable the feature. However, if you need 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.
  - After enabling custom fiscal years, when you define the first custom fiscal year, all existing forecasts, forecast history, and forecast adjustments from the first period of that year forward will be deleted. Forecasts for periods before the first custom fiscal year are not deleted and can be accessed as usual.
  - Subsequently, when you define a new custom fiscal year, any existing forecasts, forecast history, forecast adjustments, and quotas for the corresponding standard fical year are lost.
  - If you use Customizable Forecasting, reports for a period after the last defined fiscal year can be grouped only by date, not by period.
  - If you use Customizable Forecasting, to ensure your reports have the most updated amounts, view the forecast for the period included in the report before running a forecast report. 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 will not include a fiscal period columns.
- When custom fiscal years are enabled, you can't use the `FISCAL_MONTH()`, `FISCAL_QUARTER()`, or `FISCAL_YEAR()` date functions in SOQL.

SEE ALSO:

Set the Fiscal Year
Customize the Fiscal Year Structure
Customize the Fiscal Year Labels
Choosing a Custom Fiscal Year Template
Define a Custom Fiscal Year

Set the Fiscal Year

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

Warning:

- 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.

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"

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 and 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`. This option might not be available depending 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. on page 68

     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 Fiscal Years.

4. Click **Save**.

For specific information on both types of fiscal years, see Fiscal Years on page 61.

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 Fiscal Years.

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 65.

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 also 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 66. By default the number for each quarter is set by their order (the first quarter is labeled "1"); customize it by selecting 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; customize it by selecting 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 66. By default the number for each period is set by their order (the first period is labeled "1"); customize it by selecting 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 66. 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:

Fiscal Years

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 will 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 cannot do advanced customization of a fiscal year that has been created from a Gregorian calendar template. You should 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:

Fiscal Years

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 need 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 63 for more information.

Before defining or editing any custom fiscal years, be aware of its impact on forecasting, reports, and other objects by reviewing Fiscal Years on page 61.

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 67.
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: If this is the first custom fiscal year you have defined, the `Fiscal Year Start Date` and the `Week Start Date` are set to today's date and day of week. If you have already defined a custom fiscal year, they will be set to the day after the last end date of your custom fiscal years.

   To make changes other than the start date, year name, or week start day, see Customize the Fiscal Year Structure on page 64.

5. Optionally, review the fiscal year definition by clicking on **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`.

   If changing the `Fiscal Year Start Date` causes this fiscal year to overlap with the previous fiscal year, or if it creates a gap between the fiscal years, 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 if it creates 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 cannot change the start or end date of a fiscal year 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, all forecast data (including quotas, forecast history, and forecast adjustments) that are within that date range, and all forecasts for date ranges automatically adjusted as a result of that change, will be lost. This includes 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 64.

Note: Unless you specify them, the fiscal year period labels for forecasting and reporting are set by the default label values for the fiscal year periods. To change them, see Customize the Fiscal Year Labels on page 65.

Set Up Search

Customize Search Settings

To change your organization's search settings:

1. From Setup, enter *Search Settings* in the Quick Find box, then select **Search Settings**.
2. Modify the search settings for your organization.
3. Click **Save**.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To modify search settings:
- "Customize Application"

Search Settings

The search settings are:

Enable Drop-Down List for Sidebar Search
The drop-down list for sidebar search allows you to limit users' searches by object. When you select Enable Drop-Down List for Sidebar Search, a drop-down list appears in the Search section. From this list, users can select to search within tags, within a specific object, or across all objects.

Enable "Limit to Items I Own" Search Checkbox
The Limit to Items I Own checkbox allows your 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 checkbox that appears in advanced search is always available to users, regardless of this setting.

Enable Document Content Search
Enabling Document Content Search allows you to 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.

Enable Search Optimization if your Content is Mostly in Japanese, Chinese, or Korean
Enabling this checkbox optimizes search for the Japanese, Chinese, and Korean languages. It affects sidebar search and the account search for **Find Duplicates** on a lead record in sidebar search and global search. Enable this option if users are searching mostly in Japanese, Chinese, or Korean, and if the text in searchable fields is mostly in those languages.

Don't check 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 user object lookups and not to lookups for other objects.

If this setting isn't enabled, the dialog box shows a list of recently accessed user records from across your organization.

Enable English-Only Spell Correction for Knowledge Search (Beta)

If this setting is enabled, search suggests and searches alternate spellings for 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

This setting applies to article searches via the API but not to article searches in global search.

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.

Note: Global search includes auto-complete and doesn't require a search setting.

Enable Single-Search-Result Shortcut

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.

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. The current setting is in parentheses next to each object. To change this setting, select one or more objects, enter the new number of results per page, and then click **Save**. The new value must be from 5 and 50.

Lookup Settings

The Lookup Settings area allows you to enable enhanced lookups and lookup auto-completion for account, contact, user, and any custom object lookups.

SEE ALSO:

Guidelines for Making Search Faster

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.

IN THIS SECTION:

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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

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

EDITIONS

Available in: Salesforce Classic

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

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.

For example, consider an account that contains "Acme" in its `Description` field. The `Description` field isn't queried by standard lookup search, but is queried by global search and enhanced lookup search when **All Fields** is selected. So a search for Acme returns this account record only if you use either global search or enhanced lookup search with **All Fields** selected.

A few things to note about searchable fields:

- Global search finds more fields per object compared to other search types.
- By default, enhanced lookups query a limited set of fields, known as *Name* fields for each object. If your search for a record returns a large number of matches, such as a contact with a widely used name, you can instead query all searchable fields for that record to narrow your results. If available in the enhanced lookup search dialog, select **All Fields** and enter other search terms unique to the record, such as the contact's email address.
- You can't search encrypted, formula, and lookup fields.
- You can't find some objects with sidebar search or advanced search. Use global search or the search on the object's tab to find:
  - Articles
  - Chatter groups, files, topics, and people
  - Salesforce CRM Content
  - Documents
  - Price books
  - Products
  - Solutions

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.

This table shows the types of search supported for each object. 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
Asset	✓	✓			✓
Attachment	✓	✓			✓
Business Account	✓	✓	✓	✓	✓
Campaign	✓	✓	✓		✓
Calendar Event	✓	✓			✓
Case	✓	✓	✓		✓

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

Object	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search	Global Search
Person Account	✓	✓	✓	✓	✓
Price Book			✓		✓
Product			✓		✓
Question	✓	✓			✓
Quick Text	✓	✓			✓
Quote	✓	✓	✓		✓
Report	✓	✓			✓
Requested Meeting	✓	✓			✓
Reward Fund	✓	✓			✓
Reward Fund Type	✓	✓			✓
Self-Service User			✓		
Service Contract	✓	✓			✓
Skill	✓	✓			✓
Solution			✓		✓
Task	✓	✓			✓
Topic	✓	✓			✓
User	✓	✓	✓	✓	✓
Work Order	✓	✓	✓	✓	✓
Work Order Line Item	✓	✓	✓	✓	✓

Searchable Fields: Asset

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Asset Name`	✓	✓	✓
`Description`		✓	✓
`Serial Number`	✓	✓	✓
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: Attachment

Searchable Fields	Sidebar Search	Advanced Search	Global Search
Description		✓	✓
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

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search—Name Fields	Global Search and Enhanced Lookup Search—All Fields
Account Name	✓	✓	✓	✓	✓
Account Name (Local)	✓	✓	✓	✓	✓
Account Number		✓			✓
Account Site	✓	✓			✓
Billing Address		✓			✓
Description		✓			✓
D-U-N-S Number		✓			✓

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—Name Fields	Global Search and Enhanced Lookup Search—All Fields
(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 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	✓	✓		✓

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
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: Case

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)	✓	✓		✓

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
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: 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

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search—Name Fields	Global Search and Enhanced Lookup Search—All Fields
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	✓	✓			✓
Phone	✓	✓			✓

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—Name Fields	Global Search and Enhanced Lookup Search—All Fields
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

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			✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields	Sidebar Search	Advanced Search	Global Search	Content Tab
(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

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Global Search
`Billing Address`		✓		✓
`Billing Name` (First and Last)	✓	✓	✓	✓
`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		✓		✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Contract Line Item

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

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Custom Object

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.

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup ~~Search—Name~~ Fields	Global Search and Enhanced Lookup Search—All Fields
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, and rich text area		✓			✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: D&B Company

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

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	✓	✓	✓
URL		✓	✓

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

Available with a Data.com Clean license in: **Professional**, **Enterprise**, **Performance**, and **Unlimited** Editions

Searchable Fields: Dashboard

Searchable Fields	Sidebar Search	Advanced Search	Global Search
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		✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Discussion

Discussions support only standard lookup searches.

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

EDITIONS

Available in: Salesforce Classic

Available in all editions

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

Searchable Fields: External Object

An external object accesses data that's stored outside your Salesforce organization. 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 administrator for recommendations on searching your specific external system.

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

Lightning 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

Files Connect for on-premises external data sources is available for an extra cost in: **Enterprise**, **Performance**, **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)			✓	✓
`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			✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Goal

Searchable Fields	Sidebar Search	Advanced Search	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.)	✓	✓	✓

EDITIONS

Available in: Salesforce Classic

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

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

Searchable Fields: Idea

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

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Knowledge Article

Neither sidebar search nor advanced search are 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			✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields	Sidebar Search	Advanced Search	Global Search	Articles Tab
area, rich text area, email, and phone				

Searchable Fields: Lead

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Global Search
Address		✓		✓
Company	✓	✓	✓	✓
Company (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		✓		✓

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

Searchable Fields: Metric

Searchable Fields	Sidebar Search	Advanced Search	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

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: Opportunity

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search—Name Fields	Global Search and Enhanced Lookup Search—All Fields
Description		✓			✓
Opportunity Name	✓	✓	✓	✓	✓
Account 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: Order

Searchable Fields	Sidebar Search	Advanced Search	Global Search
Billing Address		✓	✓
Description		✓	✓
External Note		✓	✓
Internal Comments		✓	✓
Order Name	✓	✓	✓
Order Reference Number		✓	✓
PO Number		✓	✓
Processing Instruction		✓	✓
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

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

Searchable Fields: People

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			✓	
Email			✓	

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	People Tab
First Name			✓	✓
Last Name			✓	✓
Name			✓	✓
Nickname			✓	✓
Phone			✓	
Record ID (15 character Record ID only)			✓	
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

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: Person Account

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search—Name Fields	Global Search and Enhanced Lookup Search—All Fields
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	✓	✓			✓

EDITIONS

Available in: Salesforce Classic

Available in: **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—Name Fields	Global Search and Enhanced Lookup Search—All Fields
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

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.

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	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

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

EDITIONS

Available in: Salesforce Classic

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

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

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

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: 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	✓	✓	✓

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: 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 (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: 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 Contract

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

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Skill

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: 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: Task, Calendar Event, and Requested Meeting

Archived activities aren't searchable.

Searchable Fields	Sidebar Search	Advanced Search	Global Search
`Description` (task and 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		✓	✓

EDITIONS

Available in: Salesforce Classic

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

Searchable Fields: Topic

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

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

EDITIONS

Available in: Salesforce Classic

Available in all editions

Searchable Fields: User

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

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search—Name Fields	Global Search and Enhanced Lookup Search—All Fields
`About Me`		✓			✓
`Email`	✓	✓			✓

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—Name Fields	Global Search and Enhanced Lookup Search—All Fields
First Name	✓	✓	✓	✓	✓
Last Name	✓	✓	✓		✓
Middle Name	✓	✓		✓	✓
Name	✓	✓	✓	✓	✓
Nickname	✓	✓			✓
Phone	✓	✓			✓
Record ID (15 character Record ID only)	✓	✓			✓
Suffix	✓	✓		✓	✓
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 Order

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search—Name Fields	Global Search and Enhanced Lookup Search—All Fields
Description	✓	✓	✓	✓	✓

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—Name Fields	Global Search and Enhanced Lookup Search—All Fields
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: Work Order Line Item

Searchable Fields	Sidebar Search	Advanced Search	Standard Lookup Search	Enhanced Lookup Search—Name Fields	Global Search and Enhanced Lookup Search—All Fields
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,		✓			✓

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—Name Fields	Global Search and Enhanced Lookup Search—All Fields
email, and phone					

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.

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.

Reference the table to determine which objects you can find with a search. If an object has custom fields, you can find records of that object with the custom field values.

EDITIONS

Available in: Lightning Experience

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

Object	Fields

Account	`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)
	`Fax`
	`Phone`
	`Shipping Address`
	`Ticker Symbol`
	`Website`
	All custom fields

Asset	`Asset Name`
	`Description`
	`Serial Number`

Attachment	`Description` `Name`

Object	Fields
Campaign	`Campaign Name`

Case	`Case Comments`
	`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)

Chatter Feed	`@`*`Name`* (where *`Name`* is a username)
	`Comment Body`
	`Commenter Name`
	`File Name`
	`Group Name`
	`Links`
	`Post Body`
	`Post Origin (Person, Group, Record Name)`

Chatter Groups	`Group Description` `Group Name`

Contact	`Assistant Name`
	`Asst. Phone`
	`Department`
	`Description`
	`Email`
	`Fax`
	`First Name`
	`First Name (Local)`
	`Home Phone`
	`Last Name`
	`Last Name (Local)`
	`Mailing Address`
	`Middle Name`

Object	Fields

	`Middle Name (Local)`
	`Mobile`
	`Other Address`
	`Other Phone`
	`Phone`
	`Suffix`
	`Title`

Custom Objects and Fields	`Name` 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.
Dashboard	`Title`
Document	`Body` `Name`

File	`Body`
	`Description`
	`Extension` (such as ppt)
	`Name`
	`Owner`

Lead	`Address`
	`Company`
	`Company(Local)`
	`Description`
	`Email`
	`Fax`
	`First Name`
	`First Name (Local)`

Object	Fields
	Last Name Last Name (Local) Middle Name Mobile Phone Suffix Title
Note	Body Title
Opportunity	Description Opportunity Name Account Name
People	About Me Email First Name Last Name Name Nickname Phone Record ID (15 character Record ID only) Username
Person Account	Account Name Account Name (Local) Account Number Account Site Assistant Assistant Phone Billing Address Description Email Fax Home Phone

Object	Fields
	Mailing Address Mobile Other Address Other Phone Shipping Address Ticker Symbol Title Website
Price Book	Price Book Description Price Book Name
Product	Product Code Product Description Product Name
Report	Description Report Name
Work Order	Description Subject
Work Order Line Item	Description

Customize Users' Search Results Filters

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

   Alternatively, from the management settings for an object, go to Search Layouts, and then 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 organization 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"

Configure Lookup Dialog Search

Customize 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 Dialog Search in Salesforce Classic
Enable enhanced lookups and lookup auto-completion and customize lookup filter fields.

Configure Lookup Dialog 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 sort and filter using these columns. They are intended to provide contextual help for determining which record to associate.

Configure Lookup Dialog 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**

Administrators can configure lookups by:

- Enabling enhanced lookups
- Specifying lookup filter fields
- Enabling lookup auto-completion

IN THIS SECTION:

Enabling Enhanced Lookups

Specify Lookup 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.

Enabling 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.

Enabling Enhanced Lookups

Enable enhanced lookups so users can use wildcards in their lookups and sort, filter, and page through their results. Enhanced lookups are supported for accounts, contacts, users, opportunities, and custom 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. Currently, only account, contact, user, and custom object lookups can use this feature.
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 organization, it is also enabled for any Visualforce pages you create.

SEE ALSO:

Configure Lookup Dialog Search in Salesforce Classic

Specify Lookup 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.

1. From the management settings for accounts, contacts, opportunities, users, or custom objects, 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 should 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**.

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 Dialog Search in Salesforce Classic

Enabling 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 Dialog Search in Salesforce Classic

Configure Lookup Dialog 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 sort and filter using these columns. They are intended to provide contextual help for determining which record to associate.

Use **Search Results** under the **Search Layouts** customization setting to change which fields appear in the search results for both global search and lookup dialog search. You don't need to separately update **Lookup Dialogs**.

The order of fields in the search layout also affects the secondary field displayed in instant results. The second usable field as chosen in this step appears as the secondary field in instant results. Examples of unusable fields are HTML-formatted fields, inline image fields, 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"

Guidelines for Reducing Search Crowding

Are users reporting that records aren't appearing in their search results? Use these guidelines to help your users find the record they need.

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. However, 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 search crowding or truncation. Search crowding typically happens when:

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

- Users have limited permissions or access to records. Therefore, the records they do have access to might not be part of the results set that is filtered by access permissions.
- Users search using a term that matches a huge number of records. Because the search matches so many records, the search engine can't determine what specific record the user is searching for.

The search engine relevancy algorithms and sharing permissions decide the records returned in search results and the order of the results. To avoid search crowding and truncation:

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`.

Encourage users to narrow the search scope
When users are on the search results page, limit the search scope to the object type for the record desired. The search is rerun. Potentially, users could see more results, because the full result set limit is applied against a single object.

Create list views
Create a list view for a specific set of contacts, documents, or other object records that you search for repeatedly. List views have no limits to the number of records and have a set order. Sharing rules are also applied.

Guidelines for Making Search Faster

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Follow these guidelines to help your users find information faster.

Records are included in search results only if the object's field that contains the information matching the search term is searchable.

After a searchable object's record is created or updated, it could take about 15 minutes or more for the updated text to become searchable.

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.

Avoid making significant changes to your org at once

Creating or updating many records at the same time, such as via Data Loader, increases the amount of time required 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.

State and Country Picklists

State and Country 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 leveraged 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 Classic Mobile
- Connect Offline
- Visual Workflow or change sets
- Custom indexes

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

- 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 113.) 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.

   This step is strongly recommended 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 to see how they'll be affected by the switch.

   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, you might want to 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.

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 of 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:

- State and Country Picklists
- Edit State and Country Details
- State and Country Picklist Field-Syncing Logic
- State and Country Picklist Error Messages

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.

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.

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"

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.

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
- State and Country 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

ISO Code	Country
BF	Burkina Faso
BG	Bulgaria
BH	Bahrain
BI	Burundi
BJ	Benin
BL	Saint Barthélemy
BM	Bermuda
BN	Brunei Darussalam
BO	Bolivia, Plurinational State of
BQ	Bonaire, Sint Eustatius and Saba
BR	Brazil*
BS	Bahamas
BT	Bhutan
BV	Bouvet Island
BW	Botswana
BY	Belarus
BZ	Belize
CA	Canada*
CC	Cocos (Keeling) Islands
CD	Congo, the Democratic Republic of the
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Cote d'Ivoire
CK	Cook Islands
CL	Chile
CM	Cameroon
CN	China*
CO	Colombia
CR	Costa Rica

ISO Code	Country
CU	Cuba
CV	Cape Verde
CW	Curaçao
CX	Christmas Island
CY	Cyprus
CZ	Czech Republic
DE	Germany
DJ	Djibouti
DK	Denmark
DM	Dominica
DO	Dominican Republic
DZ	Algeria
EC	Ecuador
EE	Estonia
EG	Egypt
EH	Western Sahara
ER	Eritrea
ES	Spain
ET	Ethiopia
FI	Finland
FJ	Fiji
FK	Falkland Islands (Malvinas)
FO	Faroe Islands
FR	France
GA	Gabon
GB	United Kingdom
GD	Grenada
GE	Georgia
GF	French Guiana
GG	Guernsey

ISO Code	Country
GH	Ghana
GI	Gibraltar
GL	Greenland
GM	Gambia
GN	Guinea
GP	Guadeloupe
GQ	Equatorial Guinea
GR	Greece
GS	South Georgia and the South Sandwich Islands
GT	Guatemala
GW	Guinea-Bissau
GY	Guyana
HM	Heard Island and McDonald Islands
HN	Honduras
HR	Croatia
HT	Haiti
HU	Hungary
ID	Indonesia
IE	Ireland*
IL	Israel
IM	Isle of Man
IN	India*
IO	British Indian Ocean Territory
IQ	Iraq
IR	Iran, Islamic Republic of
IS	Iceland
IT	Italy*
JE	Jersey
JM	Jamaica
JO	Jordan

ISO Code	Country
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KH	Cambodia
KI	Kiribati
KM	Comoros
KN	Saint Kitts and Nevis
KP	Korea, Democratic People's Republic of
KR	Korea, Republic of
KW	Kuwait
KY	Cayman Islands
KZ	Kazakhstan
LA	Lao People's Democratic Republic
LB	Lebanon
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
LY	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

ISO Code	Country
ML	Mali
MM	Myanmar
MN	Mongolia
MO	Macao
MQ	Martinique
MR	Mauritania
MS	Montserrat
MT	Malta
MU	Mauritius
MV	Maldives
MW	Malawi
MX	Mexico*
MY	Malaysia
MZ	Mozambique
NA	Namibia
NC	New Caledonia
NE	Niger
NF	Norfolk Island
NG	Nigeria
NI	Nicaragua
NL	Netherlands
NO	Norway
NP	Nepal
NR	Nauru
NU	Niue
NZ	New Zealand
OM	Oman
PA	Panama
PE	Peru
PF	French Polynesia

ISO Code	Country
PG	Papua New Guinea
PH	Philippines
PK	Pakistan
PL	Poland
PM	Saint Pierre and Miquelon
PN	Pitcairn
PS	Palestine
PT	Portugal
PY	Paraguay
QA	Qatar
RE	Reunion
RO	Romania
RS	Serbia
RU	Russian Federation
RW	Rwanda
SA	Saudi Arabia
SB	Solomon Islands
SC	Seychelles
SD	Sudan
SE	Sweden
SG	Singapore
SH	Saint Helena, Ascension and Tristan da Cunha
SI	Slovenia
SJ	Svalbard and Jan Mayen
SK	Slovakia
SL	Sierra Leone
SM	San Marino
SN	Senegal
SO	Somalia
SR	Suriname

ISO Code	Country
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
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

ISO Code	Country
VG	Virgin Islands, British
VN	Vietnam
VU	Vanuatu
WF	Wallis and Futuna
WS	Samoa
YE	Yemen
YT	Mayotte
ZA	South Africa
ZM	Zambia
ZW	Zimbabwe

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. 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

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"

`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
State and Country Picklists
Integration Values for State and Country Picklists
State and Country Picklists and the Metadata API

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.

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

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

configurations, and deploy them to your production org. 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 will affect 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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

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.

- 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
- State and Country Picklists

Scan State and Country Data and Customizations

Scanning an organization for text-based state and country values reveals where and how text-based state and country data appears in existing records. For example, you can see all the ways United States is saved as a text value, such as U.S., US, America, Estados Unidos, and even misspelled entries like Untied States. In addition, scanning shows you where state and country data is used in customizations, including:

- List views
- Reports
- Validation rules
- Custom buttons and links
- Workflow rules
- Email templates
- Field sets
- Apex classes and triggers
- Visualforce pages

When the scan is complete, you receive two 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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

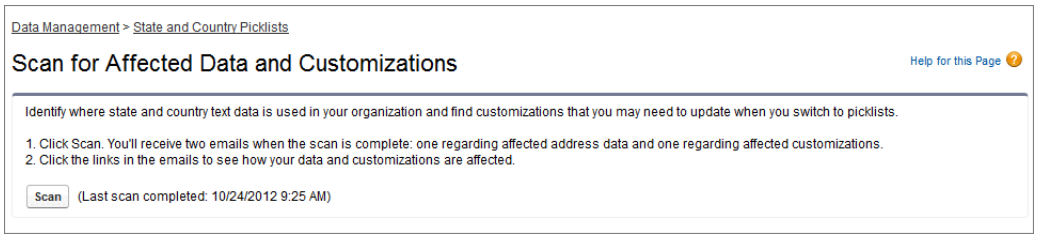
To scan state and country data and customizations:

- "Modify All Data"

  AND

  "Create Documents"

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**.

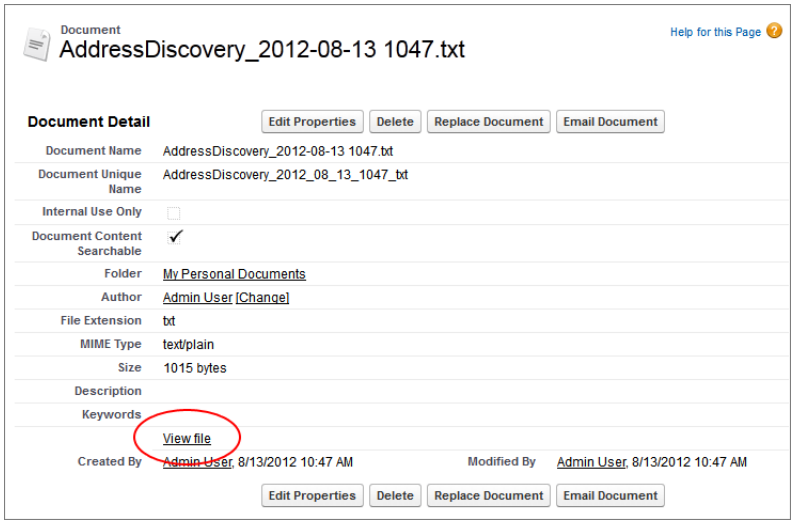


3. Wait for an email that contains the results.

   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**.



SEE ALSO:

State and Country 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, for example, you have a report that culls all of your sales reps' leads in Washington state, and 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

State and Country Picklists

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."

Before you convert state and country values in State and Country Picklists setup, configure the picklists for your org. That way, when picklists are enabled, all new and updated records use your specified integration value, helping to ensure consistent and accurate data in your org.

Convert countries first, and then states and provinces.

You can convert up to 2,000 country values and up to 2,000 state values, but state and country picklists that contain more than 1,000 states or countries can degrade performance.

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"

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 of 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 **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:

State and Country 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:

State and Country 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, as well as the state and country integration values.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Your Change	Result
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.
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:

- State and Country Picklists
- Integration Values for State and Country Picklists
- State and Country Picklist Error Messages

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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

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:

- State and Country Picklists
- Integration Values for State and Country Picklists
- State and Country Picklist Field-Syncing Logic

Customize User Interface Settings

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

1. From Setup, enter *User Interface* in the Quick Find box, then select **User Interface**.
2. Select or deselect each checkbox to modify the settings for your organization.
3. Save your changes.

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 give users the option to collapse or expand sections on their record detail pages 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 his or her settings for that tab. If your organization 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 details display an interactive overlay containing detailed information about a record when users hover the mouse 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 **View** for the record's detail page or **Edit** for the edit page. The fields displayed in the hover details are determined by the record's mini page layout. The fields that display in document hover details are not customizable. This option is enabled by default.

Note: To view the hover details for a record, users must have the appropriate sharing access to that record, and the necessary field-level security 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 the mouse over a related list hover link to display the corresponding related list and its number of records in an interactive overlay that allows users to quickly view and manage the related list items. Users can also click a related list hover link to jump down to the content of the related list without having to scroll down the page. 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 organizations 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 organization. It can take a while to retrieve data from an external system, depending on the network latency and availability of the external system. Therefore, the Enable Separate Loading of Related Lists of External Objects

option is 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: This doesn't enable enhanced lists for profiles. 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 preceded 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.

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. It dynamically determines how many tabs can display based on the width of the browser window and 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 allow users to easily print list views. If enabled, users can click the **Printable View** link from any list view to open a new browser window, displaying the current list view in a simple, 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

Available in all Editions. When enabled, the **Check Spelling** button appears in certain areas of the application where text is entered, such as sending an email, or when creating events, tasks, cases, notes, and solutions. Clicking the button checks the spelling of your text. Spell Checker does not support all the languages that Salesforce supports. For example, Spell Checker doesn't support Thai, Russian, and double-byte languages, such as Japanese, Korean, or Chinese.

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 his or her own preference for displaying the sidebar. Users can leave the sidebar visible, or they can collapse it and only show it 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 users in your org. 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 the 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 might load less quickly when this checkbox is enabled.

Enable Click-and-Create Events on Calendar Views

Allows users to create events on day and weekly calendar views by double-clicking a specific time slot and entering the details of the event 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

Allows users to create events associated with records by dragging records from list views on to weekly calendar views and entering the details of the event 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 contains all of the functionality of the original page layout editor and 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 allows you to 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 organization.

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 organization. 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
When enabled, all mail merge documents generated using Extended Mail Merge are added to the user's personal 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 organization's storage limits.

Custom Lightning Experience Navigation Menus

A navigation menu is simply a shortcut to the most-used Salesforce features. Create different menus tailored for your various types of users. What's most important to sales reps? Accounts, Events, Organizations. How about sales managers? Reports and Dashboards make the top of list. You can add, remove, and move items so that users can go to the places they use most often with a single click. Other items such as Connected apps and apps from the App Exchange are available in the App Launcher.

EDITIONS

Available in: Lightning Experience

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

IN THIS SECTION:

Lightning Experience Navigation Menu Items
Most of the items that appear in the App Launcher can appear in a navigation menu.

Create a Navigation Menu by Using the Lightning Experience Navigation Menu Wizard
The Navigation Menu wizard makes it easy to create custom Lightning Experience menus. It walks you through selecting navigation menu items and assigning user profiles.

Considerations for Lightning Experience Navigation Menus
Here's the fun part: Deciding what to put in your navigation menus. Think about these considerations when planning Lightning Experience custom navigation menus for your org.

Lightning Experience Navigation Menu Items

Most of the items that appear in the App Launcher can appear in a navigation menu.

- Your org's custom objects and apps
- Most standard objects
- Visualforce tabs
- Lightning Component tabs
- Canvas apps via Visualforcetabs
- Web tabs

Note: You can't add Connected apps like Gmail™ and Microsoft Office 365™ or Lightning Pages to navigation menus. Users access them from the App Launcher.

EDITIONS

Available in: Lightning Experience

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

Create a Navigation Menu by Using the Lightning Experience Navigation Menu Wizard

The Navigation Menu wizard makes it easy to create custom Lightning Experience menus. It walks you through selecting navigation menu items and assigning user profiles.

To start the wizard, from the Setup Quick Search box, enter **Navigation Menus**.

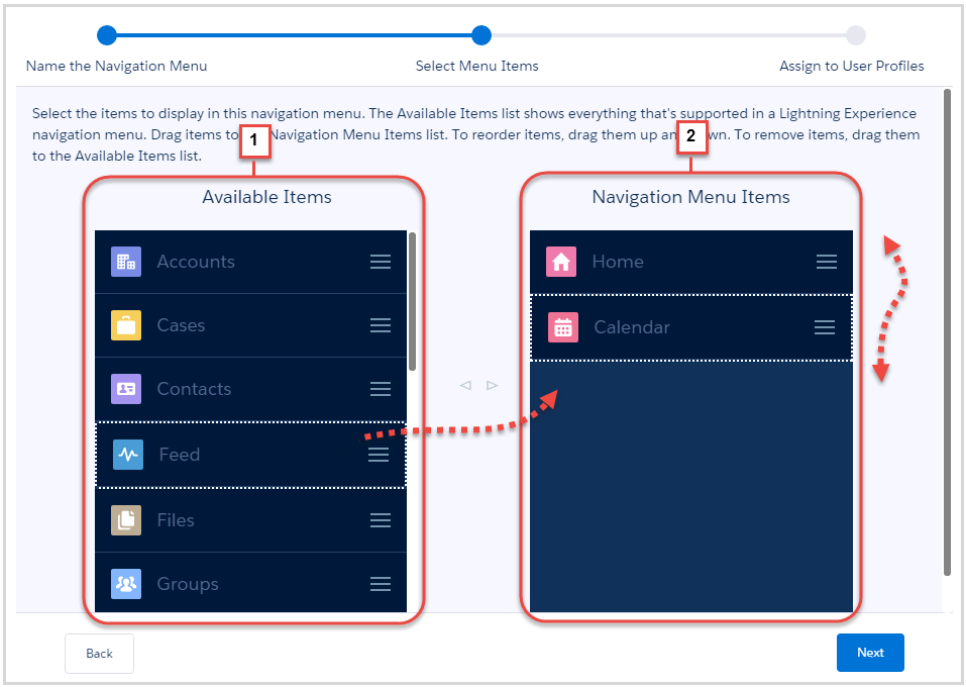
Start by naming the navigation menu.

Then the wizard displays a list of all items that can appear on a navigation menu. Drag the items you want from the available list on the left (1) to the navigation menu list on the right (2). To reorder items on the menu, drag them up and down. To remove items, drag them back to the available list on the left. When you're done, the navigation menu items list on the right reflects the order in which they appear on the navigation menu.

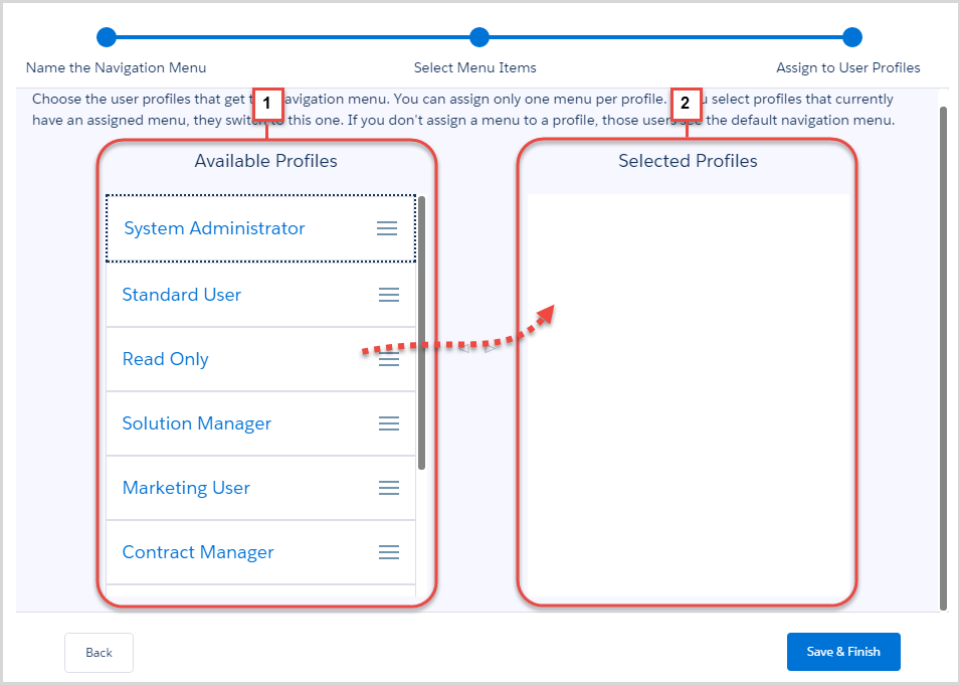
EDITIONS

Available in: Lightning Experience

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



Next, select the user profiles (1) for which you want to display this navigation menu (2).



That's it! You've created a navigation menu.

Considerations for Lightning Experience Navigation Menus

Here's the fun part: Deciding what to put in your navigation menus. Think about these considerations when planning Lightning Experience custom navigation menus for your org.

EDITIONS

Available in: Lightning Experience

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

Make a Plan

First, ask your users what their priorities are. Customizing navigation menus gives you a unique opportunity to engage with your users. Each group of users has its own priorities. Work with them to find out out which objects represent their highest priorities.

- Publish polls.
- Schedule lunch sessions. Everyone likes a free lunch and nearly everybody is happy to express their opinion.

Make creating navigation menus a part of your rollout strategy. The best time to create your menus is when you're rolling out Lightning Experience.

- See "Develop Your Rollout Strategy for Lightning Experience" in the Salesforce Help.
- See the Trailhead module "Lightning Experience Rollout." It contains many great ideas for gathering user feedback.

What objects can be added to navigation menus? Lightning Experience is a work in progress. More objects are becoming available with each release but some objects still aren't supported in Lightning Experience.

- Not all objects that appear in App Launcher can appear in a navigation menu. But it's easy to figure out which ones can. When you start the wizard, it lists all the items that you can have on a menu.

Create a master list of objects that everyone in your org wants. Then trim down the list for each user group.

- Some objects are universal for your org, such as Home, Tasks, and Feed.

- High-priority objects for one group are low priorities for other groups. Either remove the low-priority items from the user profiles or place them at the bottom of the menu.
- Are there any objects that aren't high priorities for anyone? Exclude them from the navigation menu. Users can always go to the App Launcher to get the apps they use infrequently.

Add the Apps

Clone your navigation menus..

- The easiest way to create navigation menus is to start with an existing one. Take that master list you created and add them to your first menu.
- For the rest of your navigation menus, reorder the objects according to the user profile. Or remove them altogether. Drag them from Navigation Menu Items to the Available Items list.

Add apps to your navigation menu.

- A Salesforce app is a group of tabs that work as a unit to provide application functionality. You can have custom apps that match the way your work.
- To add apps to navigation menu, each tab appears as a separate item in the available list. Make sure that you reorder the tabs so that they appear on the navigation menu next to each other.

What to Know About Assigning User Profiles

We've tried to save you from shooting yourself in the foot. If you make a mistake, you can always fall back on the default menu.

- The default navigation menu is the one that comes with Salesforce. It's the same as the Winter '16 menu: the same objects and in the same order. The default menu itself can't be edited.
- If you remove a user profile from a navigation menu without adding it to another one, the user profile is automatically assigned to the default menu.
- If you delete a custom navigation menu from a user profile without replacing it with another one, the profile switches back to the default menu.

You Can Assign a Navigation Menu to Multiple User Profiles

- You tailor navigation menus for different types of users by assigning the navigation menus to user profiles. You can assign a single navigation menu to several user profiles.
- Say that you have several groups involved with inside sales, assign all the groups the same navigation menu.

One Navigation Menu per User Profile

- A user profile can have only one navigation menu. If you assign a navigation menu to a user profile that already has a menu assigned to it, the new menu overrides the previous one.
- Users belonging to that profile immediately see the new navigation menu. Keep that in mind as you create more navigation menus. If a user suddenly sees a different navigation menu, you could get some calls.

A Few More Considerations

Navigation Menus Respect User Permissions

If a user doesn't have permission to access an object, it doesn't appear on their navigation menu.

Custom Navigation Menus Depend on Edition

The number of custom navigation menus you can have depends on your edition. You can create up to 10 navigation menus with Enterprise, Performance, and Developer Editions. If you have the Professional Edition, you can have up to five menus. If you have an Unlimited Edition, the number of navigation menus that you can have is unlimited too.

Maps and Location Services

Maps and location services uses Google Maps to display maps on standard address fields, enable 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 Salesforce1 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"

Autocomplete on Standard Addresses

You can enable autocomplete on standard addresses for all Salesforce1 users. This allows users to 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
- 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**.

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"

Note:

- Autocomplete on standard address fields is available for all versions of Salesforce1 and the Lightning Experience.

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:

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 Sharing for Reports and Dashboards

When you enable analytics 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, use filters to configure the amount of data that's captured for historical trend reporting. Then select the fields needed for historical reports.

SEE ALSO:

Upgrade the Report Wizard

Provide Convenience Features for Your Report and Dashboard Users

You can enable or disable several user interface features that may help your users get more out of reports and dashboards. These settings are for convenience and ease of use; they don't affect the data returned in your reports and dashboards.

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:

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 Salesforce1

Show your users enhanced charts in Salesforce1. 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.

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

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

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

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: Salesforce Classic

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

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

USER PERMISSIONS

To modify report and dashboard settings:
- "Customize Application"

Show Enhanced Charts in Salesforce1

Show your users enhanced charts in Salesforce1. 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.

EDITIONS

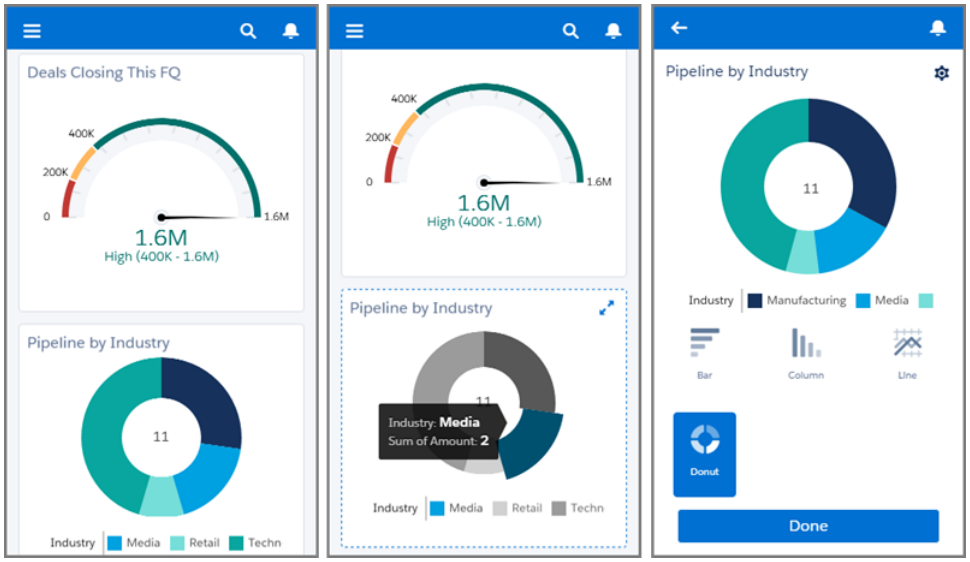
Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To modify report and dashboard settings:

- "Customize Application"



After you enable enhanced charts, everyone sees them in Salesforce1 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 Salesforce1**.
3. Click **Save**.

Before enabling enhanced charts, take note of these limitations:

- Scatter, and table charts aren't supported and appear as horizontal bar charts. Cumulative line charts aren't supported and appear as line charts.
- Enhanced charts show only the first 100 groupings in the default sort order.
- You can't post enhanced charts to Chatter.

- When you open Salesforce1, dashboards aren't automatically stored on your device for offline viewing. However, when you view a dashboard, it's saved in your device's cache so you can view it offline later.

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.

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 may be lower.

3. Click **Save**.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To modify report and dashboard settings:
- "Customize Application"

Set Up a Custom Report Type

A *report type* defines the set of records and fields available to a report based on the relationships between a primary object and its related objects. Reports display only records that meet the criteria defined in the report type.

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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create or update custom report types:

- "Manage Custom Report Types"

To delete custom report types:

- "Modify All Data"

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.

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 object, and the custom object is deleted, then the report type and any reports created from it are automatically deleted.
   - If you remove an object from a report type, all references to that object and its associated objects are automatically removed from 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.

   Note: 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 object whose Deployment Status similarly changes.

8. Click **Next**.

   Note: 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: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create or update custom report types:

- "Manage Custom Report Types"

To delete custom report types:

- "Modify All Data"

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**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create or update custom report types:
- "Manage Custom Report Types"

To delete custom report types:
- "Modify All Data"

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.

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.
   - 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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create or update custom report types:
- "Manage Custom Report Types"

To delete custom report types:
- "Modify All Data"

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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

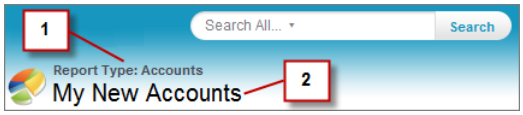
USER PERMISSIONS

To create or update custom report types:
- "Manage Custom Report Types"

To delete custom report types:
- "Modify All Data"

- 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.



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 Sharing for Reports and Dashboards

USER PERMISSIONS

To view the analytics folder sharing setting:	"View Setup and Configuration"
To modify the analytics folder sharing setting:	"Customize Application"

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

When you enable analytics 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 analytics folder sharing. If your organization existed before the Summer '13 release, follow these steps to make folder sharing available to your users.

When analytics 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 **Report and Dashboard Folder Sharing**.

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 analytics folder sharing was enabled, its properties and sharing settings are rolled back to their previous state.
- If a folder was created while enhanced analytics 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.

Set Up Historical Trend Reporting

To make historical trend reports available to your users, use 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 Item, and up to three custom objects. Historical trend reporting is available on only Collaborative forecasting, not Customizable forecasting.
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 eight fields to make available for historical trend reporting.

   These fields can be selected when creating historical trending reports.

   - For Opportunities reporting, five fields are preselected: Amount, Close Date, Forecast Category, Probability, and Stage. You can add three more.
   - For Forecasting, all eight available fields are pre-selected.

EDITIONS

Available in: both Salesforce Classic Lightning Experience

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

USER PERMISSIONS

To create, edit, and delete reports:

- "Create and Customize Reports"

  AND

  "Report Builder"

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. This includes the object's historical trending report type and any reports that have been created with it.
- 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 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: Salesforce Classic

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. 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.
3. Confirm your choice by clicking **Yes, Enable Report Builder for All Users**.

Managing Billing and Licenses

Checkout contains details about your organization's Salesforce account, including your licenses, billing information, orders, invoices, and statements.

To access Checkout, from Setup, enter *Checkout* in the Quick Find box, select **Checkout**, then choose **Proceed to Checkout**.

Note: Users with the "Manage Billing" permission have automatic access to Checkout. These users can also grant access to others within the organization Granting Checkout Access on page 155.

From Checkout, you can:

- Order more licenses and products.
- Change your billing information for an active contract.
- Change credit card information associated with an active contract.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

- View your organization's orders and invoices.
- View your previously saved quotes—both quotes you created from Salesforce and quotes created by a sales representative.
- Place orders to purchase new products.
- Contact Salesforce to request sales assistance.
- Log a case for any Checkout related questions, issues, or concerns.

For detailed instructions on using Checkout, see the Checkout User Guide.

Purchase More Licenses for Your Users

Users with Checkout enabled can add licenses for your organization at any time while a contract is in effect. If your organization doesn't have self-service access to Checkout, submit a request to your Salesforce representative.

Note: At any point during the quote creation process, you can click **Request Assistance** to contact your Salesforce account representative.

1. From Setup, enter *Checkout* in the Quick Find box, then select **Checkout** and click **Proceed to Checkout**.
2. Click **Add More Products**.
3. To see all products that your organization supports, click **All Available Products**.
4. Enter the number of license subscriptions you want to purchase.

   If licenses are purchased in the middle of a billing cycle, the subscription is prorated based on the number of days left in that billing cycle. Total Price reflects Monthly/Unit Price for the order term, which is specified above the products. For example, if an order's subscriptions start on 5/14/2013 and end on 5/7/2014, Total Price will reflect Monthly/Unit Price for 11.8 months.
5. Click **Proceed to Place Order**.
6. Review your order and payment information. Click the pencil if you need to make changes.
7. Read and confirm that you accept the Master Subscription Agreement and any other required terms and agreements.

   Depending on your contract with Salesforce and the products you're purchasing, you may have to accept Contract Special Terms or Product Specific Terms.
8. Click **Place Order**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To purchase additional user licenses:
- "Manage Billing"

SEE ALSO:

Managing Billing and Licenses
Granting Checkout Access
Removing User Licenses
Change Your Organization's Billing Information
Checkout User Guide
Converting a Trial Using Checkout

Removing User Licenses

Salesforce doesn't support using Checkout to reduce the number of licenses for your organization.

If you want to remove licenses, contact your Salesforce representative.

Note: Deactivating user accounts doesn't change the number of user licenses for which your company is billed.

SEE ALSO:

Managing Billing and Licenses
Granting Checkout Access
Purchase More Licenses for Your Users

Change Your Organization's Billing Information

To change your organization's payment and billing information, you must have access to Checkout. If your organization doesn't have self-service access to Checkout, submit a request to your Salesforce representative.

1. From Setup, enter *Checkout* in the Quick Find box, then select **Checkout**.
2. Click **Proceed to Checkout**.
3. Click **Change Contract Billing Address**.
4. Update your organization's address and contact information as necessary.
5. Click **Save**.

For detailed instructions on using Checkout, see the Checkout User Guide.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

SEE ALSO:

Managing Billing and Licenses

Changing Credit Card or Direct Debit Information

To change your credit card or direct debit information, you must have access to Checkout. If your organization doesn't have self-service access to Checkout, submit a request to your Salesforce representative.

To access Checkout, from Setup, enter *Checkout* in the Quick Find box, select **Checkout**, and then click **Proceed to Checkout**.

For specific instructions on changing your payment information in Checkout, see the Checkout User Guide.

Note: You can't pay your invoice online. Your newly-updated credit or debit card will be charged within 24 hours if there is an outstanding balance on your account. To pay an invoice via credit card, please call the Salesforce Customer Service department.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

SEE ALSO:

Managing Billing and Licenses

Viewing Credit Memos, Account Statements, and Invoices

To view your organization's credit memos, account statements, and invoices, you must have access to Checkout. If your organization doesn't have self-service access to Checkout, submit a request to your Salesforce representative.

From a credit memo, statement, or invoice details page, you can print, log cases to investigate issues, or contact Salesforce.

To access Checkout, from Setup, enter *Checkout* in the Quick Find box, select **Checkout**, and then click **Proceed to Checkout**.

Note: Your account may not have a starting balance depending on the duration of time chosen. You can open all payments, invoices, and credit memos to see more detail or to print them.

For detailed instructions on using Checkout, see the Checkout User Guide.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

SEE ALSO:

Managing Billing and Licenses

Granting Checkout Access

Users with the "Manage Billing" permission have access to Checkout when it is enabled for your organization. These users can also grant access to other users within your organization. Users with Checkout access can purchase Salesforce licenses, AppExchange app licenses, and other related products. Additionally, within Checkout, users can view the organization's quotes, installed products, orders, invoices, payments, and contracts.

To give a user access to Checkout:

1. From Setup, enter *Users* in the Quick Find box, then select **Users**.
2. Click on the appropriate user's name to open the user detail page.
3. Click **Edit**.
4. Select the Checkout Enabled checkbox. The user is notified by email when his or her Checkout account is activated and available for login.

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 grant Checkout access:
- "Manage Billing"

To edit users:
- "Manage Internal Users"

SEE ALSO:

Managing Billing and Licenses

Purchase More Licenses for Your Users

Checkout User Guide

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.

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.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

Available in: All Editions

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.

Divisions Overview

Divisions let you segment your organization's data into logical sections, making searches, reports, and list views more meaningful to users. For example, you can create a report to show the opportunities for just the North American division, allowing you to get accurate sales numbers for the North American sales team. Divisions are useful for organizations with extremely large amounts of data.

EDITIONS

Available in: Salesforce Classic

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

Note: Divisions do not restrict users' access to data and are not meant for security purposes.

Divisions can be assigned to users and to other records.

- **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 it can belong to the standard "global" division, which 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 will 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'll 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 will 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.

Area	Description
Creating new records	When you create new 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 new 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. 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, and 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 division for any detail records is determined by the previous master record.

Area	Description
	If you delete a master-detail relationship, the division for any detail records is determined by the previous master record.

SEE ALSO:

- Setting Up Divisions
- Creating and Editing Divisions
- Change the Default Division for Users
- Transferring Multiple Records Between Divisions
- Reporting With Divisions
- Administrator tip sheet: Getting Started with Divisions

Setting 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.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To create or edit divisions:

- "Modify All Data"

1. Plan which divisions you need based on how you want to segment your data.
   For example, you may want 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 additional 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 who should be able to 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, can view division fields, change the division for a record, and specify a division when creating records.

SEE ALSO:

- Divisions Overview
- Creating and Editing Divisions
- Transferring Multiple Records Between Divisions
- Change the Default Division for Users

Creating and Editing 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. Click **New** to create a divisions, or **Edit** change an existing division.
3. Enter the division name.
4. Select the checkbox to make the division active.

   Note: You cannot deactivate a division if users or lead queues are assigned to that division.
5. Click **Save**.
6. If you want to change the order that divisions appears in the Divisions picklist, click **Sort**, then to use the arrow buttons to move divisions higher or lower in the list.

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"

SEE ALSO:

- Divisions Overview
- Setting Up Divisions
- Transferring Multiple Records Between Divisions
- Change the Default Division for Users

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"

SEE ALSO:

Divisions Overview
Setting Up Divisions
Creating and Editing Divisions
Change the Default Division for Users

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**.

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"

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**.

SEE ALSO:

Divisions Overview

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:

Divisions Overview

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To limit reports by division:

- "Affected by Divisions"

How do I discontinue my service?

If the service doesn't meet your needs, you can discontinue 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.

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.

You can't customize the layout of the Home page or add custom components.

For information about enabling Account Insights, see "Account Settings" in the Salesforce Help.

Upcoming 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 user's sales team if they have an associated team. Otherwise, the chart displays opportunities owned by the user.

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

EDITIONS

Available in: Lightning Experience

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

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	✔	✔	✔

Permission or Setting	Performance Chart	Top Deals	Assistant
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			✓

Manage Users

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.

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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

The available user management options vary according to which Salesforce Edition you have.

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 organizations. Existing organizations continue to have access to the Self-Service portal.

SEE ALSO:

View and Manage Users

Licenses Overview

View and Manage Users

In the user list, you can view and manage all users in your org, partner portal, and Salesforce Customer Portal.

From Setup, enter *Users* in the Quick Find box, then select **Users**.

From the user list, you can:

- Create one user.
- 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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Contact Manager**, **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"

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.

SEE ALSO:

Deactivate (Delete) Users

Freeze or Unfreeze User Accounts

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

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

- Your *username* must be unique across all Salesforce organizations. The username must be in the format of an email address, for example, jane@salesforce.com. But the actual email in the username doesn't need to work. You *can* have the same functioning email address associated with your account across organizations—only the *username in the form of an email address* must remain unique.
- If your name includes non-English characters, add the specified language to the mail format settings within Outlook if viewing email in Outlook.
- Temporary passwords for new users expire in six months, and users must change their password the first time they log in. The login link in the email can only be used once. A user who follows the link without setting a password must have an administrator reset their password before they can log in.
- You can change a Salesforce license to a Force.com license, but you can't change a Force.com license to a Salesforce license.
- Not all options are available for all license types. For example, the `Marketing User` and `Allow Forecasting` options are not available for Force.com user licenses because the Forecasts and Campaigns tabs are not available to users with a Force.com license. Force.com user licenses are not available for Professional, Group, or Contact Manager Editions.
- In Performance, Unlimited, Enterprise, and Developer Edition organizations, you can select `Send Apex Warning Emails` to send email to the user when an application that invokes Apex uses more than half of the resources specified by the governor limits. This feature can be used during Apex code development to test the amount of resources being used at runtime.
- Temporary passwords for new users expire in six months, and users must change their password the first time they log in. The login link in the email can only be used once. A user who follows the link without setting a password must have an administrator reset their password before they can log in.

SEE ALSO:

Add a Single User

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 organizations. The username must be in the format of an email address, for example, jane@salesforce.com. But the actual email in the username doesn't need to work. You *can* have the same functioning email address associated with your account across organizations—only 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**, **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**, **Group**, **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

USER PERMISSIONS

To edit users:
- "Manage Internal Users"

SEE ALSO:

User Fields
Considerations for Editing Users
Unlock Users
SalesforceA

Considerations for Editing Users

Be aware of the following behaviors when editing users.

EDITIONS

Available in: Salesforce Classic

Available in: **Contact Manager**, **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.

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

SalesforceA

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To unlock users:

- "Manage Internal Users"

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

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.

SEE ALSO:

- Considerations for Deactivating Users
- Freeze or Unfreeze User Accounts
- Mass Transferring Records
- 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.

EDITIONS

Available in: Salesforce Classic

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

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.

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.

`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

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 her or she is assigned to.

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.

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 administrator deactivates a portal user, the administrator doesn't have the option to remove the portal user from any 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

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 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

The fields that comprise the Personal Information and other personal settings pages help to describe a user.

The visibility of fields depends on the specific page, your organization's permissions, and which edition you have.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

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.
Admin newsletter	Opt in to receive administrator-targeted promotional emails from Salesforce. This field is not available if your organization has disabled your choice to receive emails from Salesforce.
Alias	Short name to identify user on list pages, reports, and other pages where the entire name does not fit. Up to eight 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.
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 his or her Checkout account is activated and available for login. Enabling this option requires the "Manage Billing" permission.

Field	Description
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.
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 organizations using multiple currencies. This currency must be one of the active currencies for the organization.
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 organizations 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 organizations that use divisions to segment their data.

Field	Description
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 organizations that have Visualforce enabled.
Disable Auto Subscription For Feeds	Disables automatic feed subscriptions to records owned by a user. Only available in organizations 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.

Field	Description
Information Currency	The default currency for all currency amount fields in the user record. Available only for organizations 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 organizations, a user's individual Language setting overrides the organization's Default Language. Not available in Personal Edition, Contact Manager, or Group Edition™. The organization'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.
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 organization 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 organization setting.

Field	Description
`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 organization's reporting structure. 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, the user can create, edit, and delete campaigns, configure advanced campaign setup, import leads, and update campaign history via the member import wizards. Available in Professional, Enterprise, Unlimited, and Performance Editions. To use the campaign import wizards, Marketing Users must also have the Marketing User profile (or the "Import Leads" permission and the "Edit" permission on campaigns in Enterprise, Unlimited, and Performance Edition organizations). If this option isn't selected, 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.

Field	Description
	• 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. 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 organizations that use Salesforce to manage mobile configurations.
`Mobile User`	Allocates one Salesforce Classic Mobile license to the user, granting the user access to Salesforce Classic Mobile app. The number of user records enabled by this checkbox can't exceed the total number of mobile licenses your organization 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 Classic Mobile 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 Classic Mobile 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. Note: The `Mobile User` checkbox doesn't apply to the free version of Salesforce Classic Mobile because users of the free app can access Salesforce from their device without a mobile license.

Field	Description
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 organization limit.
Name	Combined first name, middle name (beta), last name, and suffix (beta) of user, as displayed on the user detail page.
Newsletter	Opt in to receive user-targeted promotional emails from Salesforce. This field is not available if your organization has disabled your choice to receive emails from Salesforce.
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.
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 Salesforce1.
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 only need 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.

Field	Description
	Portal users do not need the `Salesforce CRM Content User` license. They only need 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 can be changed by an administrator. 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.
`Salesforce1 User`	Turns on automatic redirection to the Salesforce1 mobile browser app when a user logs in to Salesforce from a supported mobile Web browser. The Salesforce1 mobile browser app option must be enabled for your organization.
`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.
`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 forVisualforce pages. This field is only visible to organizations 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 organization has. Available in Developer, Enterprise, Unlimited, and Performance Editions, only if Site.com is enabled for your organization.
`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.

Field	Description
	The number of user records with this checkbox enabled can't exceed the total number of Site.com Publisher licenses your organization has. Available in Developer, Enterprise, Unlimited, and Performance Editions, only if Site.com is enabled for your organization.
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.
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.
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."
Time-Based Token	When added, can be used to confirm the user's identity when necessary, such as when logging in from an unknown IP address. If the user has "Two-Factor Authentication for User Interface Logins" permission, the user is prompted to enter this token when logging in to Salesforce through the user interface. If the user has "Two-Factor Authentication for API Logins" permission and adds a time-based token, the user must enter this token instead of the standard security token to access the service.
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.

Field	Description
`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 Overview
- View Your Organization's Feature Licenses
- Restrict User Email Domains

Salesforce Adoption Manager

Quickly turn your mobile employees into Salesforce1 power users with Salesforce Adoption Manager. This tool trains and engages your users with intelligent email journeys aimed at driving adoption of the Salesforce1 mobile app. After inviting users to download the mobile app, Adoption Manager follows up with tips that help users get the most out of Salesforce1. It also encourages dormant Salesforce1 users to try using the app again.

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. 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. Currently, this program is about making your users more effective with the Salesforce1 mobile app.

For example, here are some amazing results from our customers when effectively using Salesforce1:

- 40% increase in employee satisfaction
- 29% faster time to find information
- 26% increase in sales productivity

What Is User Data Used for When Salesforce Adoption Manager Is Enabled?

The only change when you enable Salesforce Adoption Manager is your users receive email messages from the program, based on their usage of Salesforce1. You can review our privacy statement for more detail.

What Happens After I Activate Salesforce Adoption Manager for My Users?

Once you activate the program, it starts with a personalized invite to users to download the Salesforce1 mobile app. All emails are optimized for desktop and mobile devices. If users access the email from a desktop, they can text a download link to their mobile devices.

After users downloaded Salesforce1, 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 Salesforce1 so your company can start realizing more benefits from the product.

In the future, we plan to expand this program to help users become more effective with all Salesforce products.

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 Salesforce1.

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 Salesforce1 isn't sent to users who don't have permission to access the mobile app. Nor is it sent to users who have already installed the app.
- Five separate tips are sent to all users who downloaded Salesforce1 within the last 60 days.
- A single reminder to use Salesforce1 is sent to users who haven't accessed the mobile app for 30 days.

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?

The Marketing Cloud Support team can help confirm that the emails are being sent. 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. From Setup in the full Salesforce site, enter *Adoption* in the `Quick Find` box, select **Adoption Manager**, and then deselect `Enable Salesforce Adoption Manager`.

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.

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.

EDITIONS

Available in: Salesforce Classic

Edition requirements vary for each user, permission set, and feature license type.

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 Overview

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: For example, if you assign a Force.com user license to Employee A and a Salesforce user license to Employee B, you can give "Read" access on cases only to Employee B. Employee A's user license doesn't support standard object permissions for anything but accounts and contacts.

EDITIONS

Available in: Salesforce Classic

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: You might see other types of licenses listed if your company has purchased custom user licenses for different types of functionality. Your organization might also have other licenses that are still supported but no longer available for purchase. Contact Salesforce for more information.

The following license types are available only for organizations currently using a Customer Portal or partner portal. If you don't have a Customer Portal or partner portal but want to easily share information with your customers or partners, see Communities User Licenses on page 190.

- Customer Portal User Licenses
- Customer Portal—Enterprise Administration User Licenses
- Partner Portal User Licenses

IN THIS SECTION:

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.

SEE ALSO:

View and Manage Users

Find Company Information

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.

For information about purchasing additional user licenses, see Purchase More Licenses for Your Users on page 153 or contact Salesforce Customer Support.

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 • 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.	**Enterprise**, **Unlimited**, and **Performance** Editions
`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).	**Enterprise**, **Unlimited**, **Performance**, and **Developer** Editions

License Type	Description	Available in
	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.	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. However, these users are not entitled to some user permissions and standard apps, including standard tabs and objects such as forecasts and opportunities. 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.	**Enterprise**, **Unlimited**, **Performance**, and **Developer** Editions
`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 the same rights as Salesforce Platform users, plus they have access to an unlimited number of custom tabs. However, they are limited to the use of one custom app, which is defined as up to 10 custom objects, and they are limited to read-only access to the Accounts and Contacts objects. 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.	**Enterprise** and **Unlimited** Editions

License type	Description	Available in
`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. 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.	**Enterprise**, **Unlimited**, and **Performance** Editions
`Employee Community User`	This is an internal user license. It's designed for users to access Force.com Light application custom objects, custom tabs, Chatter (people, groups, feeds, files), and a Community that includes a Site.com site. Company Community users have read-only access to Salesforce Knowledge articles and limited access to cases for creating and reading their own cases. They can also: • Access up to 10 custom objects and 10 custom tabs • Use Content, Ideas, and Answers • Use activities, tasks, calendar, and events • Have read-only access to accounts and contacts	**Enterprise**, **Unlimited**, **Performance**, and **Developer** Editions

SEE ALSO:

User Licenses Overview

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).

EDITIONS

Available in: Salesforce Classic

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

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 need 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 links in the sidebar of the page.

Salesforce administrators can upgrade a Chatter Free license to a standard Salesforce or Chatter Only license at any time. You can't convert a standard Salesforce 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 is for users that don't have Salesforce licenses but need access to some Salesforce objects in addition to Chatter. Chatter Plus users can be Chatter moderators and have access to standard Chatter people, profiles, groups, and files pages. They also 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

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*

Chatter License Overview

This table shows the list of features that are available for Chatter External, Chatter Free, and Chatter Only 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)
Chatter Desktop client	✅	✅	✅
Use the Salesforce1 mobile app (Downloadable apps require the "API Enabled" profile permission)	✅ Downloadable app users can't access Groups or People list views.	✅	✅
Feeds	✅	✅	✅
File sharing	✅	✅	✅
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	✅	✅	✅
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			✅
Ideas and answers			✅
Reports and dashboards			✅
Tasks and activities			✅

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)
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 a Company Community license for your employees.

The Customer Community license is similar to a High Volume Customer Portal license and is well-suited for business-to-consumer communities with large numbers of external users. The Customer Community Plus license is similar to a Customer Portal — Enterprise Administration license and is well-suited for business-to-consumer communities whose users need unlimited logins to manage customer support. The Partner Community license is similar to a Gold Partner license and is well-suited for business-to-business communities, such as a partner community.

The Company Community license is used in employee communities.

EDITIONS

Available in: Salesforce Classic

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

In addition to the licenses, Communities supports all internal and portal licenses including existing Customer Portal, Authenticated Website, and partner portal licenses. Communities doesn't support the Chatter External license.

Communities licenses are associated with users, not a specific community. If needed, you can move users with these licenses between communities. Additionally, if you have unused licenses, you can assign them to users in any community in your organization.

Customer Community, Customer Community Plus, Partner Community, and Company Community licenses are also available as monthly login-based licenses. These licenses are called Customer Community Login License, Customer Community Plus Login License, Partner Community Login License, and Company Community Login License. This means that a license is consumed each time a user logs in to a community, but not when a logged-in user switches between their communities. Unused licenses expire at the end of the month. If a user with a login-based community license accesses their communities through Salesforce1, they consume a login the first time they log in or if their session times out.

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. Exceeding these limits may result in additional charges and a decrease in functionality.

Type of Community	Number of Users
Partner or Customer Community Plus	300,000
Customer	10 million

Each community has one associated Site.com site that lets you 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 Site.com site. To let Communities users without the permission edit the site, you must purchase and assign either a Site.com Publisher or a Site.com Contributor feature license, and assign a user role at the site level.

This table shows which features are available to users with Customer Community, Customer Community Plus, Partner Community, or Company Community licenses.

	Customer Community	Customer Community Plus	Partner Community	Company Community
Salesforce Standard Objects				
Accounts	✅ Read and Edit [1]	✅ Read, Create, Edit	✅ Read, Create, Edit	✅ Read, Create, Edit, Delete
Assets	✅ Read, Create, Edit	✅ Read, Create, Edit	✅ Read, Create, Edit	
Campaigns			✅ Read, Create and Edit (requires "Marketing User" permission) [2]	
Cases	✅ Read, Create, Edit [3]	✅ Read, Create, Edit	✅ Read, Create, Edit Disabled by default	✅ Read, Create, Edit, Delete
Contacts	✅	✅	✅	✅ Read, Create, Edit, Delete
Contracts	✅	✅	✅	
Documents	✅ Read Only	✅ Read Only	✅ Read Only	✅ Read, Create, Edit, Delete
Entitlements	✅ Read, Create, Edit	✅ Read, Create, Edit	✅ Read, Create, Edit	
Events & Calendar			✅ Read, Create, Edit	
Ideas	✅ Read, Create, Edit	✅ Read, Create, Edit	✅ Read, Create, Edit	✅ Read, Create
Leads			✅	
Notes and Attachments	✅ Exceptions apply [4]	✅ Only on the Attachments related list on cases [5]	✅	✅ Exceptions apply [6]
Opportunities			✅	
Orders [7]	✅	✅	✅	

	Customer Community	Customer Community Plus	Partner Community	Company Community
Price Books	✓ Read Only	✓ Read Only	✓ Read Only	
Products	✓ Read Only	✓ Read Only	✓ Read Only	
Quotes			✓	
Reports & Dashboards		✓ Read Only (by default) Create and Edit (requires user permissions) [8]	✓ Read Only (by default) Create and Edit (requires user permissions) [8]	✓ Read Only (by default) Create and Edit (requires user permissions) [8]
Service Contracts		✓ Read, Create, Edit	✓ Read, Create, Edit	
Tasks	✓ Read Only	✓ Read, Create, Edit	✓ Read, Create, Edit	✓ Read, Create, Edit
Salesforce Features, Capability, and Custom Objects				
Additional 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) 1 MB per member (login-based license) [9]
Chatter (People, Groups, Feeds, Files, Private Messages) Note: Salesforce Files Sync is not available in Communities.	✓	✓	✓	✓
Chatter Answers	✓	✓	✓	
Content (with a Salesforce CRM Content feature license)		✓ View and Upload	✓ View and Upload	✓ View, Upload, and Manage
Content (without a Salesforce CRM Content feature license)		✓ View Only	✓	✓ View, Upload, and Manage

	Customer Community	Customer Community Plus	Partner Community	Company Community
Custom Objects	✅ 10 custom objects per license (custom objects in managed packages don't count towards this limit)	✅ 10 custom objects per license (custom objects in managed packages don't count towards this limit)	✅ 10 custom objects per license (custom objects in managed packages don't count towards this limit)	✅ 10 custom objects per license (custom objects in managed packages don't count towards this limit)
Delegated Administration		✅	✅	
Knowledge	✅ Read Only	✅ Read Only	✅ Read Only	✅ Read Only
Roles and Sharing		✅	✅	✅
Salesforce1 Mobile App	✅	✅	✅	✅
Send Email			✅	✅
Workflow Approvals		✅	✅	✅ Read Only

Note:

- [1] For the Customer Community license, Read and Edit access is only on the user's own account. You can extend access to other accounts using sharing sets.
- [2] 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.
- [3] For the Customer Community license, cases can't be created on behalf of someone else.
- [4] For the Customer Community license, access to Notes and Attachments for most objects is enabled by default. For accounts and contact, this access is determined by your org's creation date. If your users with a Customer Community license can't access Notes and Attachments on accounts and contacts, contact Salesforce.
- [5] For the Customer Community Plus license, attachments are available only through the Attachments related list on Cases. Notes aren't supported.
- [6] For the Company Community license, notes and attachments are available on the Notes and Attachments related list on records like accounts, contacts and cases.
- [7] 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.
- [8] For the Customer Community Plus and Partner Community licenses 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.

- [9] For the Company Community license, the data storage limit is 20 MB per user license, and the file storage limit is 100 MB per user license.

SEE ALSO:

User Licenses Overview

Authenticated Website User Licenses

Partner Portal User Licenses

Customer Portal User Licenses

Database.com User Licenses

User License	Description	Default Number of Available Licenses
Database.com Admin	Designed for users who need to administer Database.com, or make changes to Database.com schemas or other metadata using the point-and-click tools in the Database.com Console.	Database.com Edition: 3
Database.com User	Designed for users who need Database.com access to data stored in Database.com.	Database.com Edition: 3 Enterprise, Unlimited, and Database.com Edition: 0 Contact Database.com to obtain Database.com User Licenses
Database.com Light User	Designed for users who need only Database.com access to data, need to belong to Database.com groups (but no other groups), and don't need to belong to roles or queues. Access to data is determined by organization-wide sharing defaults.	Database.com Edition: 0 Enterprise, Unlimited, and Database.com Edition: 0 Contact Database.com to obtain Database.com

EDITIONS

Available in: Salesforce Classic

Available in: **Database.com** Edition

User License	Description	Default Number of Available Licenses
		Light User Licenses

SEE ALSO:

User Licenses Overview

Service Cloud Portal User Licenses

Service Cloud Portal users have the High Volume Customer Portal license. This license gives contacts unlimited logins to your Service Cloud Portal to access customer support information. Users with this license can access accounts, assets, cases, contacts, custom objects, documents, ideas, and questions, depending on their permission settings.

The Overage High Volume Customer Portal license is the same as the High Volume Customer Portal license, except that users do not have unlimited logins. Contact Salesforce for information about the number of Customer Portal licenses you can activate.

This table lists the permissions that can be assigned to Service Cloud portal users.

EDITIONS

Available in: Salesforce Classic

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

	Create	Read	Update	Delete
Accounts		✓	✓	
Assets	✓	✓	✓	
Cases	✓	✓	✓	
Contacts	✓	✓	✓	
Custom Objects	✓	✓	✓	✓
Documents		✓		
Ideas	✓	✓		
Knowledge		✓		
Price Books		✓		
Products		✓		
Questions and Answers	✓	✓		
Solutions		✓		

SEE ALSO:

User Licenses Overview

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 Overview

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.

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.

EDITIONS

Available in: Salesforce Classic

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

	Create	Read	Update	Delete
Contracts	✓	✓	✓	✓
Documents		✓		
Ideas	✓	✓		
Knowledge		✓		
Orders	✓	✓	✓	✓
Price Books		✓		
Products		✓		
Custom Objects	✓	✓	✓	✓

SEE ALSO:

User Licenses Overview

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 190.

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 Overview

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.

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 190.

EDITIONS

Available in: Salesforce Classic

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

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		✓		
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 Overview

Partner Portal User Licenses

Partner Portal users have the Gold Partner user license. They can only access Salesforce using the partner portal.

EDITIONS

Available in: Salesforce Classic

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

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 190.
- 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 Partner Portal users.

	Create	Read	Update	Delete
Accounts	✓	✓	✓	
Approvals		✓		
Assets	✓	✓	✓	
Campaigns [1]	✓	✓	✓	
Cases	✓	✓	✓	
Contacts	✓	✓	✓	
Contracts	✓	✓	✓	✓
Custom Objects	✓	✓	✓	✓
Documents		✓		
Ideas	✓	✓	✓	
Knowledge		✓		
Leads	✓	✓	✓	
Opportunities	✓	✓	✓	
Orders	✓	✓	✓	✓
Price Books		✓		

	Create	Read	Update	Delete
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 Overview

Permission Set Licenses

A permission set is a convenient way to assign users specific settings and permissions to use various tools and functions.

EDITIONS

Available in: Salesforce Classic

The availability of each permission set license depends on the edition requirements for permission sets and the related feature.

IN THIS SECTION:

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.

Available Permission Set Licenses

For each permission set license available for purchase, see which permissions it enables you to assign to your users.

View Your Organization's Permission Set Licenses

View the permission set licenses your organization has purchased to know what you have available to assign to your users.

Assign a Permission Set License to a User

Some permissions require you to assign a permission set license to the user and then add the permissions to permission sets.

Remove a Permission Set License from a User

First remove or modify the relevant assigned permission sets that require the license, and then remove the assigned permission set license.

SEE ALSO:

Find Company Information

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.

As additive licenses, permission set licenses don't limit functionality. With permission set licenses, you can assign more permissions to users than their user license supports.

After you assign a permission set license to a user, assign the appropriate permissions to that user through a permission set—not a profile.

Example:

- Before you can assign a permission set with the "Use Identity Connect" permission to a user, assign an Identity Connect permission set license to that user.
- Before you can assign a permission set with "Read" or "Edit" on orders to a user with a Force.com user license, assign an Orders Platform permission set license to that user. You can assign those permissions to a user with a Salesforce user license without a permission set license, because it's already enabled as part of the user license.

EDITIONS

Available in: Salesforce Classic

The availability of each permission set license depends on the edition requirements for permission sets and the related feature.

SEE ALSO:

Permission Set Licenses

Available Permission Set Licenses

For each permission set license available for purchase, see which permissions it enables you to assign to your users.

Permission Set License	User Permissions Included	Object Permissions Included
Employee Community User for Force.com	"Allow View Knowledge"	"Create" and "Read" on Cases
Files Connect for on-premises external data sources	"Files Connect On-premises"	
Identity Connect	"Use Identity Connect"	
Orders Platform	• "Activate Contracts" • "Delete Activated Contracts" • "Activate Orders" • "Edit Activated Orders"	"Create," "Read," "Edit," and "Delete" on: • Contracts • Price Books • Products

EDITIONS

Available in: Salesforce Classic

The availability of each permission set license depends on the edition requirements for permission sets and the related feature.

Permission Set License	User Permissions Included	Object Permissions Included
	• "Create Reduction Orders"	• Orders
Sales Console User	"Sales Console"	

SEE ALSO:

- Assign a Permission Set License to a User
- User Permissions
- Assign Permission Sets to a Single User
- Permission Set Licenses

View Your Organization'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
- Available Permission Set Licenses
- Assign a Permission Set License to a User

EDITIONS

Available in: Salesforce Classic

Available in: **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

Some permissions require you to assign a permission set license to the user and then add the permissions to permission sets.

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 to that user, and then click **Save**.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To assign a permission set license:

- "Manage Users"

After you've assigned a permission set license to a user, add the related permission to a permission set, and then assign that permission set to the user.

SEE ALSO:

- Permission Set Licenses
- Remove a Permission Set License from a User
- Permission Sets
- Assign Permission Sets to a Single User

Remove a Permission Set License from a User

First remove or modify the relevant assigned permission sets that require the license, and then remove the assigned permission set license.

1. Identify the permission that requires the permission set license 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 **Edit Assignments**.
6. Deselect the appropriate permission set license.
7. Click **Save**.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To remove a permission set license:

- "Manage Users"

SEE ALSO:

- Permission Set Licenses
- View Your Organization's Permission Set Licenses
- Assign a Permission Set License to a User

Feature Licenses Overview

A feature license entitles a user to access an additional feature that 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

EDITIONS

Available in: Salesforce Classic

Edition requirements vary for each feature licenses.

Depending on the features that are enabled for your organization, you might be able to assign more than one type of feature license to your users.

SEE ALSO:

- View and Manage Users
- Purchase More Licenses for Your Users
- Find Company Information

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.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To view feature licenses:

- "View Setup and Configuration"

SEE ALSO:

- Feature Licenses Overview
- Available Feature Licenses
- Enable a Feature License for a User
- View and Manage Users
- Purchase More Licenses for 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.

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**.

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"

SEE ALSO:

- Edit Users
- Add a Single User
- Feature Licenses Overview
- Available Feature Licenses
- View Your Organization's Feature Licenses

Available Feature Licenses

Assign one or more of these additional feature licenses to users so they can access features not included in their user license.

EDITIONS

Available in: Salesforce Classic

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

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, import leads, and update campaign history via the member import wizards.
`Mobile User`	Access Salesforce Classic Mobile. The `Mobile User` checkbox doesn't apply to the free version of Salesforce Classic Mobile because users of the free app can access Salesforce from their device without a mobile license.
`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 Overview

EDITIONS

Available in: Salesforce Classic

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 organization 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 organization 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 organization 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 organization 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 organization's list users can add or export up to 2,000 records until that date. If the organization 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 organization 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 Organization's Usage-Based Entitlements

Look at your company's usage-based entitlements to know which resources your organization is entitled to.

Usage-based Entitlement Fields

SEE ALSO:

Find Company Information

View and Manage Users

View Your Organization's Usage-Based Entitlements

Look at your company's usage-based entitlements to know which resources your organization 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 Overview

Usage-based Entitlement Fields

EDITIONS

Available in: Salesforce Classic

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 organization is entitled to a resource.

EDITIONS

Available in: Salesforce Classic

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

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 organization can use. If Frequency is Monthly, the month begins on your Start Date.

Column name	Description
`Amount Used`	The amount of this resource that your organization is using.
`Last Updated`	The most recent date and time when Salesforce took a snapshot of your organization's usage for this resource.

For more information about resources your organization is entitled to, contact Salesforce.

SEE ALSO:

Usage-based Entitlements Overview

View Your Organization'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 536.
- 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 539.
- User password resets—Reset the password for specified users. See Reset Passwords for Your Users on page 213.
- 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 167.

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.

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. 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.

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 set password policies:
- "Manage Password Policies"

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 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 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. d. Click **Unlock**. This button is only available when a user is locked out.

Field	Description
`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 organization uses the Microsoft Input Method Editor (IME) with the input mode set to Hiragana, when you type ASCII characters they're converted into Japanese characters in normal text fields. However, the IME does not work properly in fields with obscured text. If your organization'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: • 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.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To reset passwords:

- "Reset User Passwords and Unlock Users"

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.
- 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:

Passwords

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:
- "Manage Internal 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 Salesforceadmins, 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 Experience

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

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.

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.
3. To return to your administrator account, click *User's Name* > **Logout**.

SEE ALSO:

Control Login Access

View and Manage Users

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"

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.

Note: When delegating administration, keep the following in mind. Delegated administrators:

- Can't assign profiles or permission sets with the "Modify All Data" permission.
- Need access to custom objects to access the merge fields on those objects from formulas.
- Can't modify permission sets.

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"

To delegate administration of particular objects, use object permissions, such as "View All" and "Modify All," instead.

SEE ALSO:

Define Delegate Administrators

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.


Walk Through It: Delegate Administration


Walk Through It: Delegate Administration in Lightning Experience

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.

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"

SEE ALSO:

Delegate Administrative Duties

Topics and Tags Settings

With or without Chatter enabled, administrators can enable topics for objects, letting users 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, leads, opportunities, orders, solutions, custom objects, and English articles.

Administrators set up and manage personal and public tags by:

- Enabling tags for accounts, activities, assets, campaigns, cases, contacts, contracts, dashboards, documents, events, leads, notes, opportunities, reports, solutions, tasks, and any custom objects (except relationship group members)
- Adding tags to the sidebar for their users
- Deleting 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.

Administrators can enable topics for accounts, assets, campaigns, cases, contacts, contracts, 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.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To enable topics for objects:
- "Customize Application"

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.

Enabling Tags

EDITIONS

Available in: Salesforce Classic

Tag settings available in: **All** Editions

USER PERMISSIONS

To modify tag settings:
- "Customize Application"

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 should display tags in a tag section at the top of record detail pages. The tag section is the only way that a user can add tags to a record.

   For example, if you only select account page layouts, users in your organization can only tag account records. Additionally, if you only select account page layouts for personal tags and not public tags, users can only tag account records with personal tags.
4. Click **Save**.

When enabling tags, keep these guidelines in mind

- You can also add them to page layouts by editing a layout directly. Note, however, that tags can't be added 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

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.

EDITIONS

Available in: Salesforce Classic

Tag settings available in: **All** Editions

USER PERMISSIONS

To modify tag settings:
- "Customize Application"

SEE ALSO:

Topics and Tags Settings

Deleting Personal Tags for Deactivated Users

Your organization can have a maximum of 5,000,000 personal and public tags applied to records across all users. If your organization is approaching this limit, you can 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.

EDITIONS

Available in: Salesforce Classic

Personal Tag Cleanup available in: **All** Editions

USER PERMISSIONS

To delete personal tags for deactivated users:
- "Customize Application"

SEE ALSO:

Topics and Tags Settings

Securing Data Access

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

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.

Revoking Permissions and Access

SEE ALSO:

Profiles

Permission Sets

Field-Level Security Overview

Sharing Settings

User Permissions and Access

User permissions and access settings are specified in profiles and permission sets. It's important to understand the differences between profiles and permission sets so you can use them effectively.

User permissions and access settings specify what users can do within an organization. For example, 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 additional permissions as needed.

EDITIONS

Available in: Salesforce Classic

The available permissions and settings vary according to which Salesforce edition you have.

The following 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	✅	✅
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

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Your organization includes several standard profiles, in which you can edit a limited number of settings. In Enterprise, Performance, Unlimited, and Developer Edition organizations, you can use standard profiles or create custom profiles. In custom profiles, you can edit all permissions and settings except the user license. In Contact Manager, Group, and Professional Edition organizations, 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.

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 organization 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 new 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.

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: **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** 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.

Assigning Record Types and Page Layouts 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.

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.

SEE ALSO:

Enhanced Profile User Interface Overview

Enhanced Profile User Interface Overview

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

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To enable the enhanced profile user interface:

- "Customize Application"

App and System Settings in the Enhanced Profile User Interface

In the enhanced profile user interface, administrators can easily navigate, search, and modify settings for a single profile. Permissions and settings are organized into pages under app and system categories, which reflect the rights users need to administer and use app and system resources.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **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.

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 Call Center 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 custom permissions, type *cust*, then select Custom Permissions. And so on.

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"

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

Assigning 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.
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.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To edit record type and page layout access settings:

- "Manage Profiles and Permission Sets"

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?

Assigning 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.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view login hour settings:
- "View Setup and Configuration"

To edit login hour settings:
- "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 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

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 Classic Mobile app can bypass IP ranges that are defined for profiles. Salesforce Classic Mobile 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 Classic Mobile on page 758 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: **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** 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: **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** 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.

Viewing and Editing 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.

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
- Viewing and Editing 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: **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

USER PERMISSIONS

To edit 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

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit profiles:

- "Manage Profiles and Permission Sets"

  AND

  "Customize Application"

Setting	To view or edit, go to
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
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.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To assign page layouts in profiles:

- "Manage Profiles and Permission Sets"

7. Click **Save**.

SEE ALSO:

Work in the Original Profile Interface

Viewing and Editing 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

Available in: Salesforce Classic

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

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.

   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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To assign record types to profiles:
- "Customize Application"

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

Assigning 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

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.

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"

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 Classic Mobile app can bypass IP ranges that are defined for profiles. Salesforce Classic Mobile 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 Classic Mobile on page 758 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

Standard Profiles

Every organization includes standard profiles that you can assign to users. In standard profiles, you can edit some settings.

Every organization includes standard profiles. In Enterprise, Unlimited, Performance, and Developer Edition, you can use standard profiles or create, edit, and delete custom profiles. In organizations where you can't create custom profiles (such as Contact Manager, Group, and Professional Edition), 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.

EDITIONS

Available in: Salesforce Classic

Your edition determines which standard profiles are available.

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 any quota, override forecasts, and view any forecast.
Standard Platform User	Can use custom Force.com AppExchange apps developed in your organization 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 organization 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 organization's setup. Can view, but not manage, campaigns. Can create, but not review, solutions. Can edit personal quota and override forecasts.

Profile Name	Available Permissions
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, import leads, create letterheads, create HTML email templates, manage public documents, and update campaign history via the import wizards. 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.
Read Only	Can view the organization'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

Profile Name	Available Permissions
	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 only 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 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.
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

Profile Name	Available Permissions
	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**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** 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"

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.
- 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.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create, edit, and delete profile list views:

- "Manage Profiles and Permission Sets"

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.
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

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 new profiles, save time by cloning existing profiles and customizing them.

Tip: If you clone profiles to enable certain permissions or access settings, consider enabling them using permission sets. For more information, see Permission Sets.

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**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create profiles:
- "Manage Profiles and Permission Sets"

SEE ALSO:

Profiles

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:

- 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**

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

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

Additional permission sets available for an extra cost in **Professional** Edition

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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view tab settings:
- "View Setup and Configuration"

To edit tab settings:
- "Manage Profiles and Permission Sets"

IN THIS SECTION:

Tab Settings
Tab settings specify whether a tab appears in the All Tabs page or is visible in its associated app. Tab settings labels in permission sets differ from the labels in profiles.

SEE ALSO:

Profiles

Tab Settings

Tab settings specify whether a tab appears in the All Tabs page or is visible in its associated app. Tab settings labels in permission sets differ from the labels in profiles.

EDITIONS

Available in: Salesforce Classic

Available in all editions except **Database.com**

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. Individual users can

Enabled Settings in Permission Sets	Enabled Setting in Profiles	Description
		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.

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: **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** 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**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit session and password settings in profiles:
- "Manage Profiles and Permission Sets"

To set password policies:
- "Manage Password Policies"

SEE ALSO:

Password Policy Fields in Profiles

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 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 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: 1. Enter *Users* in the Quick Find box.

Field	Description
	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 organization uses the Microsoft Input Method Editor (IME) with the input mode set to Hiragana, when you type ASCII characters they're converted into Japanese characters in normal text fields. However, the IME does not work properly in fields with obscured text. If your organization'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.

Watch a Video Tutorial: Who Sees What: Permission Sets

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.

Note: In Contact Manager, Group, and Professional Editions, you can create one permission set.

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.

Use permission sets to grant access among logical groupings of users, regardless of their primary job function. For example, let's say you have an Inventory custom object in your organization. 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.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Additional permission sets available for an extra cost in **Professional** Edition


Walk Through It: Create, Edit, and Assign a Permission Set


Walk Through It: Create, Assign, and Add a Permission Set in Lightning Experience

SEE ALSO:

- Edit Permission Sets from a List View
- Assign Permission Sets to a Single User
- Permission Sets Considerations

Create Permission Sets

You can clone a permission set or create a new one. A cloned permission set starts with the same user license and enabled permissions as the permission set that it's cloned from. A new permission set starts with no user license selected and no permissions enabled.


Walk Through It: create, edit, and assign a permission set

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Additional permission sets available for an extra cost in **Professional** Edition

USER PERMISSIONS

To create permission sets:

- "Manage Profiles and Permission Sets"

User Licenses in Permission Sets

When creating a permission set, you can select a specific user license or **--None--**.

If you're selecting a specific license, select the license that matches the users who use the permission set. For example, if you plan to assign this permission set to users with the Salesforce license, select Salesforce.

If you plan to assign this permission set to multiple users with different licenses, select **--None--** for no user license. With this option, you can assign the permission set to any users whose license allows the enabled permissions. For example, if you plan to assign the permission set to users with the Salesforce license as well as users with the Salesforce Platform license, select **--None--**.

Note:

- Permission sets with no user license don't include all possible permissions and settings.
- You can only assign a permission set with no license to users whose licenses allow the enabled permissions and settings. For example, if you create a permission set with no user license and enable "Author Apex," you can't assign that permission set to users with the Salesforce Platform user license because the license doesn't allow that permission.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Additional permission sets available for an extra cost in **Professional** Edition

Permission Sets Considerations

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

In Enterprise, Performance, Unlimited, Developer, and Database.com editions, you can create up to 1,000 permission sets. In Contact Manager, Group, and Professional Editions, you can create one permission set.

In Group, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com editions, organizations can have more permission sets if they're added as part of an installed managed package that's publicly listed on AppExchange. In this case, organizations can have up to 1,500 permission sets.

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.

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

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Additional permission sets available for an extra cost in **Professional** Edition

Triggers always fire on trigger events (such as `insert` or `update`), regardless of permission settings.

SEE ALSO:

How is record type access specified?

User Licenses in Permission Sets

Object Permissions

Using Permission Set Lists

To view the permission sets in your organization, from Setup, enter *Permission Sets* in the Quick Find box, then select **Permission Sets**. In the permission sets list page, you can:

- Show a filtered list of permission sets by selecting a view from the drop-down list
- Create a list view or edit an existing view
- Delete a list view by selecting it from the drop-down list and clicking **Delete**
- Create a permission set by clicking **Create**
- Print a list view by clicking .
- Refresh the list view by clicking 
- Edit permissions directly in a list view
- View or edit a permission set by clicking its name
- If it's not assigned to any users, remove a permission set by clicking **Del**

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

Additional permission sets available for an extra cost in **Professional** Edition

USER PERMISSIONS

To view permission sets, and print permission set lists:

- "View Setup and Configuration"

To delete permission sets and permission set list views:

- "Manage Profiles and Permission Sets"

Create and Edit Permission Set List Views

You can create and edit permission set list views to show a list of permission sets with specific fields and permissions. For example, you could create a list view of all permission sets in which "Modify All Data" is enabled.

1. In the Permission Sets 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 to search for and select the setting you want.
   b. Choose a filter operator.
   c. Enter the value that you want to match.

      Tip: To show only permission sets with no user license, enter *`User License`* for the `Setting`, set the `Operator` to *`equals`*, and enter `""` in the `Value` field.

   d. To specify another filter condition, click **Add Row**. You can specify up to 25 filter condition rows.
4. Under Select Columns to Display, specify the settings that you want to appear as columns in the list view. You can add up to 15 columns.
   a. From the Search drop-down list, select a setting type.
   b. Enter the first few letters of the setting you want to add and click **Find**.

      Note: If the search finds more than 500 values, no results appear. Refine your search criteria to show fewer results.
5. Click **Save**, or if you're cloning an existing view, rename it and click **Save As**.

SEE ALSO:

Edit Permission Sets from a List View

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Additional permission sets available for an extra cost in **Professional** Edition

USER PERMISSIONS

To create, edit, and delete permission set list views:

- "Manage Profiles and Permission Sets"

Edit Permission Sets from a List View

You can change permissions in up to 200 permission sets directly from the list view, without accessing individual permission sets.

Note: Use care when editing permission sets with this method. Making mass changes can have a widespread effect on users in your organization.

1. Select or create a list view that includes the permission sets and permissions you want to edit.
2. To edit multiple permission sets, select the checkbox next to each one you want to edit. If you select permission sets on multiple pages, the selections on each page are remembered.
3. Double-click the permission you want to edit. For multiple permission sets, double-click the permission in any of the selected permission sets.
4. In the dialog box that appears, enable or disable the permission. In some cases, changing a permission can also change other permissions. For example, if "Manage Cases" and "Transfer Cases" are enabled in a permission set and you disable "Transfer Cases," then "Manage Cases" is also disabled. In this case, the dialog box lists the affected permissions.
5. To change multiple permission sets, select **All** *n* **selected records** (where *n* is the number of permission sets you selected).
6. Click **Save**.

If you edit multiple permission sets, only the permission sets that support the permission you are editing change. For example, let's say you use inline editing to enable "Modify All Data" in ten permission sets, but one permission set doesn't have "Modify All Data." In this case, "Modify All Data" is enabled in all the permission sets, except the one without "Modify All Data."

Any changes you make are recorded in the setup audit trail.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Additional permission sets available for an extra cost in **Professional** Edition

USER PERMISSIONS

To edit multiple permission sets from the list view:

- "Manage Profiles and Permission Sets"

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.


Walk Through It: create, edit, and assign a permission set

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Additional permission sets available for an extra cost in **Professional** Edition

USER PERMISSIONS

To delete permission sets and edit permission set properties:

- "Manage Profiles and Permission Sets"

About App and System Settings in Permission Sets

In permission sets, permissions and settings are organized into app and system categories, which 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

Additional permission sets available for an extra cost in **Professional** Edition

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.

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

Additional permission sets available for an extra cost in **Professional** Edition

USER PERMISSIONS

To search permission sets:
- "View Setup and Configuration"

If no results appear in a search:

- Be sure that the search term has at least three consecutive characters that match the object, setting, or permission name.
- Be sure that the search term is spelled correctly.
- The permission, object, or setting you're searching for may not be available in the current organization.

- The item you're searching for may 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.

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

Additional permission sets available for an extra cost in **Professional** Edition

USER PERMISSIONS

To edit assigned app settings:

- "Manage Profiles and Permission Sets"

Assigning 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**.

SEE ALSO:

How is record type access specified?

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To assign record types in permission sets:

- "Manage Profiles and Permission Sets"

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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

- 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 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:

Assigning Record Types and Page Layouts in the Enhanced Profile User Interface

Assign Record Types to Profiles in the Original Profile User Interface

Assigning 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**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **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

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Additional permission sets available for an extra cost in **Professional** Edition

Permission Set Assigned Users Page

From the Assigned Users page, you can view all users who are assigned to a permission set, assign additional users, and remove user assignments.

To view all users that 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

Additional permission sets available for an extra cost in **Professional** Edition

USER PERMISSIONS

To view users that are assigned to a permission set:

- "View Setup and Configuration"

Assign Permission Sets to a Single User

You can assign permission sets or remove permission set assignments for a single user from the user detail page.

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**.
4. To assign a permission set, select it from the Available Permission Sets box and click **Add**. To remove a permission set assignment, select it from the Enabled Permission Sets box and click **Remove**.

   Note:

   - The Permission Set Assignments page shows permission sets with no associated license and 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 and permission sets with no associated license to that user.

     If you assign a permission set with no associated user license, all of its enabled settings and permissions must be allowed by the user's license, or the assignment will fail.

   - Some permissions require users to have *permission set licenses* before the user can have those permissions. For example, if you add the "Use Identity Connect" permission to the "Identity" permission set, only users with the Identity Connect permission set license can be assigned the "Identity" permission set.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Additional permission sets available for an extra cost in **Professional** Edition

USER PERMISSIONS

To assign permission sets:

- "Assign Permission Sets"

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
- SalesforceA
- User Licenses in Permission Sets
- Assign a Permission Set to Multiple Users

Assign a Permission Set to Multiple Users

From any permission set page, you can assign the permission set to one or more users.

- Walk Through It: assign a permission set

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

Additional permission sets available for an extra cost in **Professional** Edition

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

Additional permission sets available for an extra cost in **Professional** Edition

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

Additional permission sets available for an extra cost in **Professional** Edition

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, 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 additional access.

SEE ALSO:

- User Permissions and Access
- Walk Through It: create, edit, and assign a permission set
- Assign Permission Sets to a Single User

What Determines Field Access?

Several factors control whether users can view and edit specific fields in Salesforce. You can control users' access to fields at the record type, user, or field level.

- **Page layouts**—Set whether fields are visible, required, editable, or read only for a particular record type.
- **Field-level security**—Further restrict users' access to fields by setting whether those fields are visible, editable, or read only. These settings override field properties set in the page layout if the field-level security setting is more restrictive.
- **Permissions**—Some user permissions override both page layouts and field-level security settings. For example, users with the "Edit Read Only Fields" permission can always edit read-only fields regardless of any other settings.
- **Universally required fields**—Override field-level security or any less-restrictive settings on page layouts by making a custom field universally required.

After setting these items, confirm users' access to specific fields using the field accessibility grid.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Page layouts are not available in **Database.com**

SEE ALSO:

- Modifying Field Access Settings

Verify Access for a Particular Field

See whether access to a field is restricted and at what level— record type, user profile, or field.

1. Navigate to the fields area of the appropriate object:
   - For Knowledge validation status picklists, from Setup, enter *Validation Statuses* in the Quick Find box, then select **Validation Statuses**.
2. Select a field and click **View Field Accessibility**.
3. Confirm that the field access is correct for different profiles and record types.
4. Hover over any field access setting to see whether the field is required, editable, hidden, or read only based on the page layout or field-level security.
5. Click any field access setting to change it.

To verify field accessibility by a specific profile, record type, or field, from Setup, enter *Field Accessibility* in the Quick Find box, then select **Field Accessibility**. From this page, choose a particular tab to view and then select whether you want to check access by profiles, record types, or fields.

Note: In this user interface, you can't check access for permission sets.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view field accessibility:
- "View Setup and Configuration"

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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **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"

- Alternatively, you can select the `Choose a different page layout` radio button to assign a different page layout to the profile and record type combination.

SEE ALSO:

What Determines Field Access?

Field-Level Security Overview

Note: Who Sees What: Field-level Security

Watch how you can restrict access to specific fields on a profile by profile basis.

EDITIONS

Available in: Salesforce Classic

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

Field-level security settings let administrators restrict users' access to view and edit specific fields in:

- Detail and edit pages
- Related lists
- 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 apply. For example, if a field is required in the page layout and read-only in the field-level security settings, the field-level security overrides the page layout and the field will be read-only for the user.

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 any of the following ways:

- For multiple fields on a single permission set or profile
- For a single field on all profiles

After setting field-level security for users, you can:

- Create page layouts to organize the fields on detail and edit pages.

  Tip: Use field-level security as the means to restrict users' access to fields; then use page layouts primarily to organize detail and edit pages within tabs. This reduces the number of page layouts for you to maintain.

- Verify users' access to fields by checking the field accessibility.
- Customize search layouts to set the fields that display 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 always read-only on detail pages and not available on edit pages. They may also be visible to users even though they reference fields that your users cannot see. Universally required fields always display 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.

SEE ALSO:

Administrator tip sheet: Tips & Hints for Page Layouts and 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: **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

USER PERMISSIONS

To set field-level security:
- "Manage Profiles and Permission Sets"

  AND

  "Customize Application"

Setting 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.
5. Click **Save**.

EDITIONS

Available in: Salesforce Classic

Available in: **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

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: **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

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	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 view all users in the organization, especially 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.

EDITIONS

Available in: Salesforce Classic

Available in all editions

"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

Salesforce user security is an intersection of sharing, and user and object permissions. In some cases, such as in end-user record level access, it is advantageous to use sharing to provide access to records. In other cases, such as when delegating record administration tasks like transferring records, cleansing data, deduplicating records, mass deleting records, and delegating workflow approval processes, it is advantageous to override sharing and use permissions to provide access to records.

The "Read," "Create," "Edit," and "Delete" permissions respect sharing settings, which control access to data at the record level. The "View All" and "Modify All" permissions override sharing settings for specific objects. Additionally, the "View All Data" and "Modify All Data" permissions override sharing settings for *all* objects.

The following table describes the differences between the security models.

EDITIONS

Available in: Salesforce Classic

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

	Permissions that Respect Sharing	Permissions that Override Sharing
Target audience	End-users	Delegated data administrators
Where managed	"Read," "Create," "Edit," and "Delete" object permissions; Sharing settings	"View All" and "Modify All"
Record access levels	Private, Read-Only, Read/Write, Read/Write/Transfer/Full Access	"View All" and "Modify All"
Ability to transfer	Respects sharing settings, which vary by object	Available on all objects with "Modify All"
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.
Group access levels determined by	Roles, Roles and Subordinates, Roles and Internal Subordinates, Roles, Internal and	Profile or permission sets

	Permissions that Respect Sharing	Permissions that Override Sharing
	Portal Subordinates, Queues, Teams, and Public Groups	
Private record access	Not available	Available on private contacts, opportunities, and notes and attachments with "View All" and "Modify All"
Ability to manually share records	Available to the record owner and any user above the record owner in the role hierarchy	Available on all objects with "Modify All"
Ability to manage all case comments	Not available	Available with "Modify All" on cases

Field Permissions

Field permissions specify the access level for each field in an object. In permission sets and the enhanced profile user interface, the setting labels differ from those in the original profile user interface and in field-level security pages for customizing fields.

Access Level	Enabled Settings in Permission Sets and Enhanced Profile User Interface	Enabled Settings in Original Profile and Field-Level Security Interfaces
Users can read and edit the field.	`Read` and `Edit`	`Visible`
Users can read but not edit the field.	`Read`	`Visible` and `Read-Only`
Users can't read or edit the field.	None	None

EDITIONS

Available in: Salesforce Classic

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

SEE ALSO:

- Field-Level Security Overview
- 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

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. You can access queues from list views, and queue members can jump in to take ownership of any record in a queue. Queues are available for cases, leads, orders, custom objects, service contracts, and knowledge article versions. 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

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.

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**

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

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.
`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.

Field	Description
`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.
`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

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

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**

SEE ALSO:

Organization-Wide Sharing Defaults

Set Your Organization-Wide Sharing Defaults

External Organization-Wide Defaults Overview

External organization-wide defaults provide separate organization-wide defaults for internal and external users. They simplify your sharing rules configuration and improve recalculation performance. Additionally, 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

EDITIONS

Available in: Salesforce Classic

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

- 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

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.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To set default sharing access:
- "Manage Sharing"

Access Level	Description
`Controlled by Parent`	Users can perform actions (such as view, edit, delete) on a record on the detail side of a master-detail relationship if they can perform the same action on all associated master records. 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

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.

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"

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.

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"

SEE ALSO:

User Role Hierarchy

Role Fields

The fields that comprise a role entry have specific purposes. Refer to this table for descriptions of each field and how it functions in a role.

The visibility of fields depends on your organization's permissions and sharing settings.

Field	Description
`Case Access`	Specifies whether users can access other users' cases that are associated with accounts the users own. This field 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.
`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.

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
	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?

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 others users
- To add multiple users to a Salesforce CRM Content library
- To assign users to specific actions in Salesforce Knowledge

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

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.

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
	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 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. 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.

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"

`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 automatically 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.
   - 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.

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"

SEE ALSO:

What Is a Group?

Sharing Records with Manager Groups

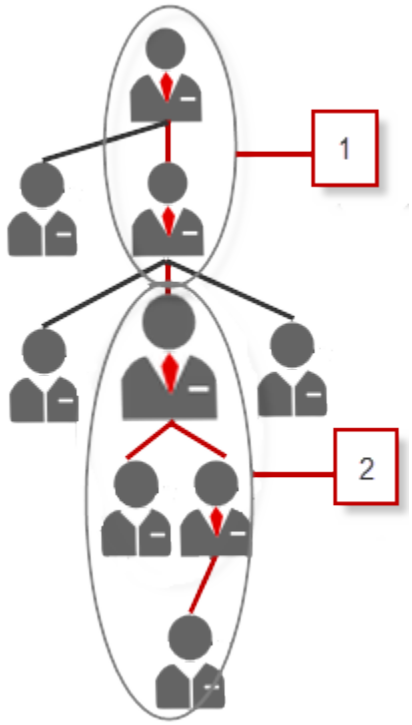
Share records up or down the management chain using sharing rules or manual sharing.

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.

EDITIONS

Available in: Salesforce Classic

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



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

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 asset records
Campaign sharing rules	Campaign owner or other criteria, including campaign record types or field values	Individual campaign records
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

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 **Professional** Edition for an additional cost, and **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Type	Based on	Set Default Sharing Access for
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
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
User sharing rules	Group membership or other criteria, including username and whether the user is active	Individual user records
User provisioning request sharing rules	User provisioning request owner, only; criteria-based sharing rules aren't available	Individual user provisioning request records

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 Overview

Sharing Rule Considerations

Criteria-Based Sharing Rules Overview

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." You can create a criteria-based sharing rule that shares 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 Metadata API to create criteria-based sharing rules starting in API version 24.0.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Accounts, Opportunities, Cases, and Contacts are not available in **Database.com**

- 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 create criteria-based sharing rules for accounts, opportunities, cases, contacts, leads, campaigns, 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 won't share records with "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. 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.

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
	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.

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:

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create sharing rules:
- "Manage Sharing"

- `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 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.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit sharing rules:
- "Manage Sharing"

6. Click **Save**.

SEE ALSO:

Sharing Rules

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.

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"

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.
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 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.

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 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**.

SEE ALSO:

Sharing Rules

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 Categories

Editing Account Territory Sharing Rules

For account territory sharing rules, you can edit the sharing access settings, but no other settings.

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**.

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 Categories

Creating Contact Sharing Rules

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:

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"

- `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 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.

Access Setting	Description
Read Only	Users can view, but not update, records.
Read/Write	Users can view and update records.

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"

6. Click **Save**.

SEE ALSO:

Sharing Rules

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.

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 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.

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 Categories

Editing Opportunity 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 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**.

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 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 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**.

SEE ALSO:

Sharing Rules

Sharing Rule Categories

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit sharing rules:

- "Manage Sharing"

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.
7. Depending on the rule type you selected, do the following:

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"

- `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 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**.

SEE ALSO:

Sharing Rules

Sharing Rule Categories

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"

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**.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To create sharing rules:
- "Manage Sharing"

SEE ALSO:

Sharing Rules

Sharing Rule Categories

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 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 Categories

Creating 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.
6. Select a rule type.

EDITIONS

Available in: Salesforce Classic

Available in: **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.

10. Click **Save**.

Editing Order 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 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**.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To edit sharing rules:
- "Manage Sharing"

Creating User Provisioning Request Sharing Rules

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.

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"

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 Categories

Editing User Provisioning Request Sharing Rules

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.

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 Categories

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To edit sharing rules:

- "Manage Sharing"

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

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

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.
- 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.

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

SEE ALSO:

Understanding User Sharing

Restoring User Visibility Defaults

Controlling Who Community or Portal Users Can See

Understanding User Sharing

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.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Manual sharing available in: Salesforce Classic

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

"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

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.

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"

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.

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.

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"

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.

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**.

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:

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

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**.

EDITIONS

Available in: Salesforce Classic

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

Controlling Who Community or Portal Users Can See

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.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To set Community and Portal User Visibility:

- "Manage Sharing"

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.

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.

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.

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.

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"

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.

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**.

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"

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

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.
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.
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.

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"

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.

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.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

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

EDITIONS

Available in: Salesforce Classic

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

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.

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 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 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.

  Note: Professional Edition customers cannot manage users this way because custom profiles are not enabled in Professional Edition organizations.

- 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

The organization-wide sharing default for contacts is not available to organizations that have person accounts enabled.

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 Settings

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 usually automatically 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: You don't need to recalculate each time you edit or create a sharing rule. Only use the Recalculate buttons on the Sharing Rules related lists if sharing rule updates have failed or are not working as expected. The administrator will receive a notification email if sharing rule updates have failed.

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 rule will be calculated as well. You'll 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 Sharing Rules

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

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.

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

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 (Pilot)

When you create, edit, or delete a sharing rule, recalculation runs to update record access in the organization. This operation can take some time if you have many users and a lot of data. The object-specific share locks feature enables you to make changes to a sharing rule for other objects, without waiting for recalculation across all objects to complete. Depending on the object, sharing rule type, and target group of the users, you can make changes to sharing rules on another object or the same object via the UI or API.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

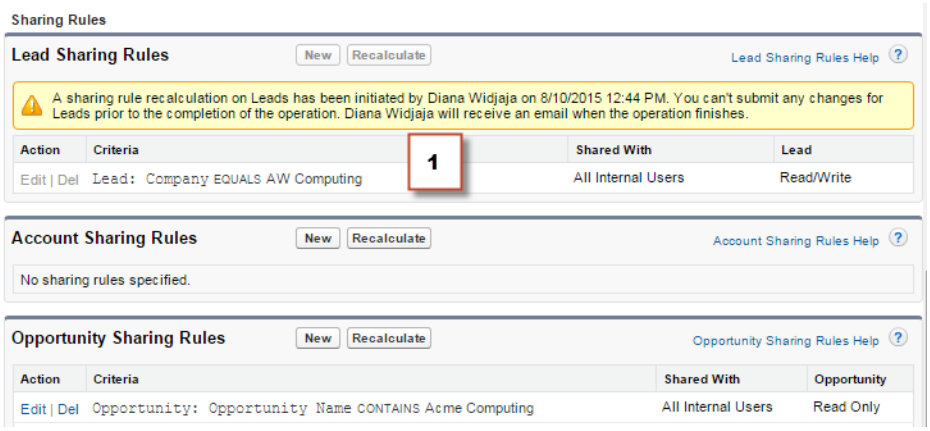
Note: We provide this feature to selected customers through a pilot program that requires agreement to specific terms and conditions. To be nominated to participate in the program, contact Salesforce. Because pilot programs are subject to change, we can't guarantee acceptance. This pilot feature isn't generally available, as referenced in this document 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 features.

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 organization.

Criteria-based and ownership-based sharing rules

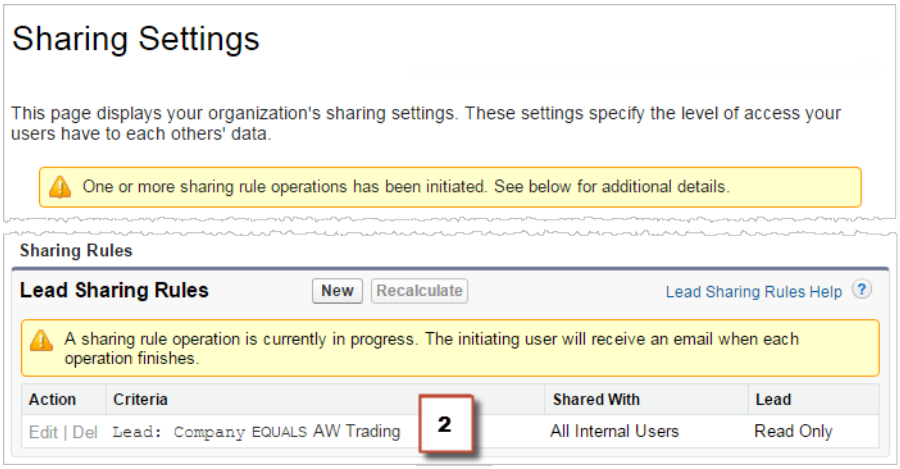
Recalculation is run if a sharing rule has changed or when you click the **Recalculate** button on the Sharing Settings page. Clicking this button locks sharing rules for that object (1), but you can still make changes to sharing rules for another object.

Note: You don't need to recalculate each time you edit or create a sharing rule. Only use the Recalculate buttons on the Sharing Rules related lists if sharing rule updates have failed or are not working as expected. The administrator will receive a notification email if sharing rule updates have failed.

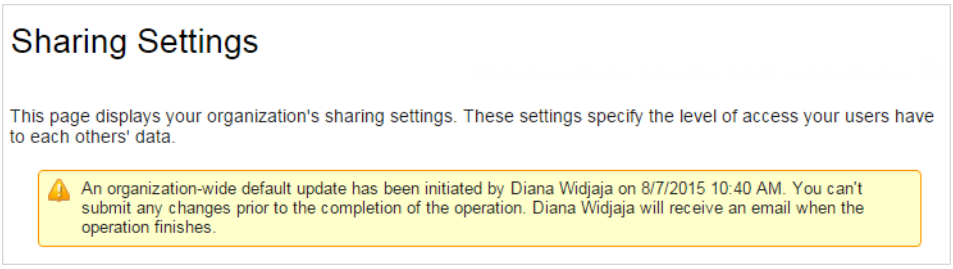


When an ownership-based sharing recalculation is in progress, you can't create, edit, or delete ownership-based sharing rules for an object that targets the affected group of users. For example, let's say you're creating an ownership-based lead sharing rule targeting all internal users. You can create, update, or delete another ownership-based sharing rules for leads targeting all internal users only after the recalculation finishes. You'll receive an email notification when the recalculation is complete. However, you can still create another ownership-based sharing rules for leads targeting any other public group except the All Internal Users group, while the recalculation from the creation of the first sharing rule is still in progress.

When a criteria-based sharing recalculation is in progress, you can't edit or delete that rule (2). But you can simultaneously create, edit, or delete any other criteria-based or ownership-based sharing rule.



You can't modify the organization-wide defaults when a recalculation is running and vice versa.

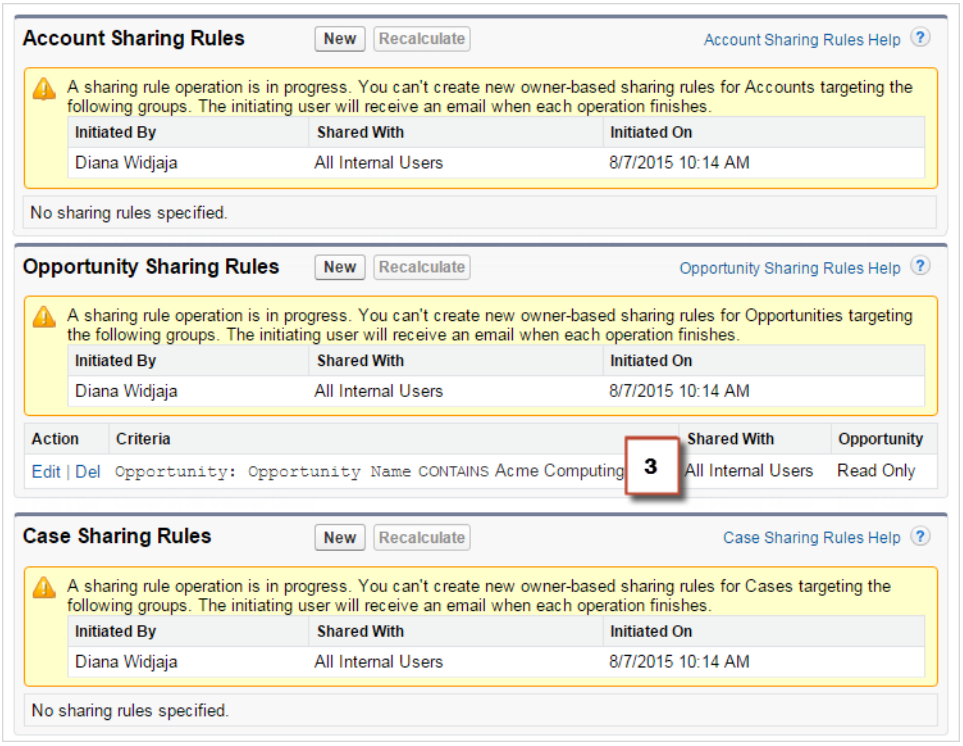


Account, cases, contacts, and opportunities

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 and editing account sharing rules 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. Note that locks are not shared across objects, except in the case of accounts and associated account children.

Note: Clicking the **Recalculate** button for any of these four objects' sharing rules prevents anyone from making changes to any sharing rules for those objects until recalculation is completed.

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 belonging to any of these objects, you can make changes to a criteria-based sharing rule (3) belonging to those objects.



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.

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

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

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:

Securing Data Access

Resolving Insufficient Privileges Errors

EDITIONS

Available in: Salesforce Classic

Available in: **All Editions**

Most Insufficient Privileges errors are caused by a missing permission or sharing setting that's preventing you from accessing a record or performing a task, like running a report.

A user might not have the right access on different levels, such as an object, a record, or a process. For example, a user's profile might be preventing the user from accessing the account object, or a user's role might be preventing the user from accessing a case record. You might also see this error when you click a link to a record or a Visualforce page tab to which you don't have access.

Most cases can be resolved by using the Sharing button on the record detail page, which enables you to share the record to another user if necessary. 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: Who Sees WhatWatch this video series to understand how to grant users the access they need.

Resolve Permission and Object-Level Access Errors

Insufficient Privileges errors might be caused by a lack of object and user permissions. You can troubleshoot this type of errors through a user's 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. For example, 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.

      Or if the user is trying to run a report, he or she might not have "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 take action accordingly.

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"

SEE ALSO:

Resolving Insufficient Privileges Errors

Permission Sets

User Permissions and Access

Profiles

Resolve Record-Level Access Errors

Insufficient Privileges errors might be caused by your sharing settings, such as roles or sharing rules.

To verify if your error is at record-level, follow these steps. Alternatively, 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 that of the user whose record is being accessed.

      For example, 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. If the user should have gotten access via a sharing rule, review your sharing rules.

   The user might have been unintentionally left out from a sharing rule.

   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) that the user should belong to for that sharing rule.

3. Verify your sales teams.

   If your organization uses teams for accounts, opportunities, or cases, you might have missed the user when setting up the teams. Review your teams to determine if the user should have gotten 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.

   The user might have gained access via a manual share but lost this access because the record owner changed, causing the manual share to be automatically dropped. The manual share might have been removed using the **Sharing** button on the record detail page. 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.

   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, the user might be missing from the territories or the record might not be under the correct territory where the user is a member. Otherwise, you must be a forecast manager, `Forecast managers can manage territories` is selected, and you are working below your position in the territory hierarchy.

SEE ALSO:

Resolving Insufficient Privileges Errors

User Role Hierarchy

Sharing Rules

Resolve Process-Level Access Errors

Insufficient Privileges errors might be caused by a validation rule.

To resolve Insufficient Privileges errors, you would typically determine if they are caused by misconfigured permission sets, profiles , or sharing settings. Otherwise, you might want to review your organization's validation rules.

1. Review your validation rules.

   A validation rule might be preventing 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 if the user must gain access through it.

SEE ALSO:

Resolving Insufficient Privileges Errors

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"

Record Access FAQ

- Why does a user have access to an account?

Why does a user have access to an account?

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:

Securing Data Access

Resolving Insufficient Privileges Errors

Managing Folders

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"
To create, edit, and delete public report folders:	"Manage Reports in Public Folders"
To create, edit, and delete public dashboard folders:	"Manage Dashboards" AND "View All Data"

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Report folders not available in: **Contact Manager**, **Group**, and **Personal** Editions

A *folder* is a place where you can store reports, dashboards, documents, or email templates. Folders can be public, hidden, or shared, and can be set to read-only or read/write. You control who has access to its contents based on roles, permissions, public groups, and license types. You can make a folder available to your entire organization, or make it private so that only the owner has access.

- To access 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

Creating and Editing Folders

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"
To create, edit, and delete public report folders:	"Manage Reports in Public Folders"
To create, edit, and delete public dashboard folders:	"Manage Dashboards" AND "View All Data"

EDITIONS

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

Report folders not available in: **Contact Manager**, **Group**, and **Personal** Editions

Document folder restriction not available in: **Developer** Edition

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 Sharing for Reports and Dashboards and Share a Report or Dashboard Folder.

6. Click **Save**.

SEE ALSO:

Managing Folders

Deleting Folders

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"
To create, edit, and delete public report folders:	"Manage Reports in Public Folders"
To create, edit, and delete public dashboard folders:	"Manage Dashboards" AND "View All Data"

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Report folders not available in: **Contact Manager**, **Group**, and **Personal** Editions

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

Filing Items in Folders

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"
To create, edit, and delete public report folders:	"Manage Reports in Public Folders"
To create, edit, and delete public dashboard folders:	"Manage Dashboards" AND "View All Data"

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Report folders not available in: **Contact Manager**, **Group**, and **Personal** Editions

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

Import Your Data

Importing Overview

You can import up to 50,000 records into Salesforce from an existing data source.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the unified Data Import Wizard. (Individual import wizards open in small pop-up windows, while the unified wizard opens in a full browser with dataimporter.app at the end of the URL.) To start using the unified wizard, 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 the comma delimited text format (.csv), such as Excel or GoldMine.

Note: If commas are not appropriate for your locale, use a tab or other delimiter.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Your edition determines the types of objects you can import.

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 organization

Which records can be imported?

Type of record	Import record limit	Users with access	Overview topic
Business accounts and contacts owned by you	500 at a time	All users	What Is Imported for Business Accounts and Contacts?
Business accounts and contacts owned by different users	50,000 at a time	Administrators; Users with the "Modify All Data" permission	What Is Imported for Business Accounts and Contacts?
Person accounts owned by you	50,000 at a time	All users	What Is Imported for Person Accounts?

Which records can be imported?

Type of record	Import record limit	Users with access	Overview topic
Person accounts owned by different users	50,000 at a time	Administrators; Users with the "Import Person Accounts" permission	What Is Imported for Person Accounts?
Leads	50,000 at a time	Administrators; Users with "Read", "Create", and "Edit" on leads and the "Import Leads" permission	What is Imported for Leads?
Campaign members	50,000 for importing leads as new campaign members and updating the status of existing campaign members.	Administrators; Marketing users (or users with the "Import Leads" permission and the "Edit" permission on campaigns) can import new leads as campaign members. Users also need the "Read" permission on contacts to use the campaign update wizard to make existing leads and contacts campaign members.	What is Imported for Campaign Members?
Custom objects	50,000 at a time	Administrators; Users with the "Modify All Data" permission	What Is Imported for Custom Objects?
Solutions	50,000 at a time	Administrators; Users with the "Import Solutions" permission	What Is Imported for Solutions?
Assets Cases Campaigns Contracts Documents Opportunities Products	These records cannot be imported via the import wizards.		

For information on field accessibility and how different field type values are imported, see Notes on Importing Data on page 349.

Note: Relationship group members can't be imported.

SEE ALSO:

- Data Import Wizard
- Deciding on A Method for Importing Data
- Undoing an Import

Deciding on A Method for Importing Data

Learn about your options for importing data into of 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 editions except Database.com	Up to 50,000	Yes	No	Internal	An in-browser wizard that imports your organization's accounts, contacts, leads, solutions, and custom objects. Read more.
Data Loader	Enterprise, Unlimited, Performance, Developer, and Database.com Editions	Between 5,000 and 5 million	Yes	Yes	External	Data Loader is an application for the bulk import or export of data. Use it to insert, update, delete, or export Salesforce records. Read more.
Import My Accounts & Contacts wizard	Contact Manager, Group, Professional, Enterprise, Unlimited, Performance, and Developer Editions	Up to 500 records for an individual user Up to 50,000 records for multiple users	Yes	No	Internal	An in-browser wizard that imports personal contacts and accounts from various data sources, like Act!™, Gmail™, and Outlook®.

SEE ALSO:

- Data Import Wizard
- Importing Overview

What Is Imported for Business Accounts and Contacts?

The import wizards for contacts and business accounts allow you to match records in a variety of ways in order to prevent duplicates. Contacts can be matched by Salesforce ID, name, or email. Business accounts can be matched by Salesforce 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 will also be matched by Salesforce ID.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Organization import not available in: **Personal** Edition, **Database.com**

Matching by Name and Site

If you choose to match contacts by name and business accounts by name and site (which are the recommended options), the import wizards automatically create a business account for each unique business account name and site in the import file. They also create 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 already exists in the system, and you have read/write access to the record, the wizards add your import data to the existing data in Salesforce. In addition, if a business account or contact name in your import file is similar to an existing business account or contact name, the import data is added 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 selected, the Salesforce ID will be 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, then that record will be updated in Salesforce. Note that record IDs are case-sensitive and must match exactly.

Overwriting Existing Account Values

The wizards never overwrite your existing business account fields unless you check the `Overwrite existing account values` checkbox in the wizard. With this box checked, you can insert or update existing business account fields with new data. However, you cannot use this checkbox to update existing field data with blank values. With this box unchecked, the wizard updates any empty business account fields, but does not touch any fields with existing 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 organizations, 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.

SEE ALSO:

- Data Import Wizard
- Importing My Contacts from Outlook or ACT!
- Import My Contacts from Other Sources
- Deciding on A Method for Importing Data
- Importing Overview

What is Imported for Leads?

You can import data into the standard lead fields and into any custom lead fields you may have, even if a particular 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, or email. Choosing a matching type sets the criteria for avoiding duplicate leads. For example, if you are matching by email and a lead in your source file has the same email as a lead in Salesforce, then that lead will be updated in Salesforce. If you are not matching by email and a lead in your source file has the same email as a lead in Salesforce, then a new lead will be created.

The wizards never overwrite your existing lead fields unless you check the `Overwrite existing lead values` checkbox in the wizard. With this box checked, you can insert or update existing lead fields with new data. However, you cannot use this checkbox to update existing field data with blank values. With this box unchecked, the wizard updates any empty lead fields, but does not touch any fields with existing data.

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 new lead in Salesforce. You can merge leads after they are imported.

SEE ALSO:

Data Import Wizard

Deciding on A Method for Importing Data

What is Imported for Campaign Members?

- **Data Import Wizard** - For each lead in your import file, this wizard imports the lead, associates the lead with a campaign, and inserts a `Member Status` value for the lead in that campaign. You can import data into the standard lead fields and into any custom lead fields, even if a particular field is hidden or read only in your page layout or field-level security settings. If you have duplicate leads in your import file, the wizard does not merge them. In addition, if any of the imported leads match an existing lead, the wizard does not merge the duplicate data into one lead.
- **Campaign Update Wizard** - For each contact or lead in your import file, this wizard updates only the `Member Status` value of the matching contact or lead in Salesforce. You cannot add new leads or contacts, nor can you update any other fields in the existing lead or contact records.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

SEE ALSO:

Data Import Wizard

Deciding on A Method for Importing Data

What Is Imported for Custom Objects?

The Data Import Wizard for custom objects allows you to prevent the creation of 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**, **Group**, **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To import custom objects:
- "Modify All Data"

Matching by Name

When you select this option, the import wizard will detect existing records in Salesforce that have the same name. Note that this type of matching is not case-sensitive - for example, names that begin with a capital letter will be matched with the same name that begins with a lowercase letter. If necessary, scan and standardize your custom object 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 import wizard will detect existing records in Salesforce that have the same Salesforce ID. Note that Salesforce IDs are case-sensitive and must match exactly. Salesforce IDs can be obtained 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 import wizard will detect existing records in Salesforce that have the same external ID. Note that this operation is not case-sensitive - for example, "ABC" will be matched with "abc". However, there is an exception: if the custom field has the separate "Unique" attribute and the case-sensitive option for that attribute is selected, uppercase and lowercase letters will not be considered identical.

If necessary, scan and standardize your external ID values before performing the import to prevent unintended matches.

When matching by external ID, if the import wizard finds duplicate records, only the first three duplicate records are reported to you in the confirmation email.

Ignoring or Updating Matching Records

When the import wizard detects existing records in Salesforce that match according to the field you have chosen, you can choose one of the following actions:

- **Do not update existing records and only insert new records** - If there are records in your file that are new and do not match any existing records, then insert them into Salesforce. Also, ignore any records in your file that match an existing record, and do nothing to the existing record.
- **Update existing records and do not insert any new records** - If there are records in your file that match an existing record, then update the existing record. Also, ignore any records in your file that do not match an existing record, and do not insert them as new records.
- **Update existing records and insert new records** - If there are records in your file that are new and do not match any existing records, then insert them into Salesforce. Also, if there are records in your file that match an existing record, then update the existing record.

Note: Custom objects with two master-detail relationships cannot be imported using the import wizard.

SEE ALSO:

Data Import Wizard

Deciding on A Method for Importing Data

What Is Imported for Solutions?

The Data Import Wizard allows you to prevent the creation of 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 will detect existing solutions in Salesforce that have the same title. Note that this type of matching is not case-sensitive - for example, titles that begin with a capital letter will be 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 import wizard will detect existing records in Salesforce that have the same Salesforce ID. Note that Salesforce IDs are case-sensitive and must match exactly. Salesforce IDs can be obtained 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 import wizard will detect existing records in Salesforce that have the same external ID. Note that this operation is not case-sensitive - for example, "ABC" will be matched with "abc". However, there is an exception: if the custom field has the separate "Unique" attribute and the case-sensitive option for that attribute is selected, uppercase and lowercase letters will not be considered identical.

If necessary, scan and standardize your external ID values before performing the import to prevent unintended matches.

When matching by external ID, if the import wizard finds duplicate records, only the first three duplicate records are reported to you in the confirmation email.

Ignoring or Updating Matching Records

When the import wizard detects existing records in Salesforce that match according to the field you have chosen, you can choose one of the following actions:

- **Do not update existing records and only insert new records** - If there are records in your file that are new and do not match any existing records, then insert them into Salesforce. Also, ignore any records in your file that match an existing record, and do nothing to the existing record.

- **Update existing records and do not insert any new records** - If there are records in your file that match an existing record, then update the existing record. Also, ignore any records in your file that do not match an existing record, and do not insert them as new records.
- **Update existing records and insert new records** - If there are records in your file that are new and do not match any existing records, then insert them into Salesforce. Also, if there are records in your file that match an existing record, then update the existing record.

SEE ALSO:

Data Import Wizard

Deciding on 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. Field access is determined by user permissions, page layout assignments, and field-level security settings.

  Field-level security is available in Enterprise, Unlimited, Performance, and Developer Editions only.

- **New Values for Picklists and Multi-Select Picklists**—If your import file contains data to be displayed in picklists or multi-select picklists, the wizards warn you when you attempt to import a new picklist value that does not match any valid picklist values. If you ignore the warning, the new value is automatically added to the imported record. Your administrator can later edit the field to add the necessary values. Note that the import wizards do not allow you to import more than 100 new picklist or multi-select picklist values for any field during a single import.

  If your organization uses the Translation Workbench, the import wizards look for matching translated values before creating new inactive picklist values.

- **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.

- **Universally Required Fields**—You must include universally required fields in your import files or the import will fail.

SEE ALSO:

Data Import Wizard
Deciding on A Method for Importing Data
Importing Overview

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

Import My Accounts and Contacts

For personal imports, all amounts in new accounts and contacts are imported in your personal currency. When import updates amounts in existing records, the amounts in your file are converted from your personal currency to the currency of the account or contact.

For example, suppose your personal currency is U.S. dollars, and your import file has 100 as the annual revenue of an existing account with `Account Currency` of euros. The new `Annual Revenue` value of the account is EUR 92, assuming a conversion rate of 0.92 and "EUR" as the currency code for euros.

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.
- **Using one currency for accounts and contacts** - If you are importing accounts and contacts, the `Currency ISO Code` column applies to both an account and its associated contact. You cannot specify different currencies for associated accounts and contacts.
- **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.

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.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

1. Use your existing software to create a data export file.
   - Exporting from ACT!
   - Exporting from LinkedIn®
   - Exporting from Outlook
   - Exporting from GoldMine 4.0
   - Exporting from GoldMine 5.0
   - Exporting from Palm Desktop
   - 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 Preparing Your Data for Import on page 356.
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!

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 are not appropriate for your locale, use a tab or other delimiter.

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.

EDITIONS

Available in: Salesforce Classic

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

Exporting from Outlook

Export data directly from Microsoft® Outlook® in a CSV (comma-separated values) format. Then import that data into Salesforce.

1. In Outlook, navigate to the export feature.
2. Choose **Comma Separated Values (Windows)** and click **Next**.

   Note: If commas are not appropriate for your locale, use a tab or other delimiter.

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 GoldMine 4.0

GoldMine 4.0 allows you to export contact data in a text format that can be imported. Additionally, you can export GoldMine 4.0 notes for import into Professional, Enterprise, Unlimited, Performance, and Developer Edition organizations.

- Exporting Contacts from GoldMine 4.0
- Exporting Notes from GoldMine 4.0

Exporting Contacts from GoldMine 4.0

To export contact data from GoldMine 4.0, follow these steps:

1. Launch GoldMine 4.0.
2. Choose **Export Records** from the **Tools** menu.
3. Select **Export to a new file** and **DBF file**, and click **Next**.
4. In the list of GoldMine Fields on the left side of the dialog, select all of the fields, and click **Add Field**. Then click **Next**.
5. Choose the location for the export file, and click **Next**.
6. Select **No** when asked if you want to save these settings, and click **Next**.
7. Click **Finish**.
8. After the export finishes, locate the exported file and change its file extension from .dbf to .csv. The file is now ready for import into Salesforce.

Exporting Notes from GoldMine 4.0

Before importing your GoldMine 4.0 notes into Salesforce, you must import your GoldMine 4.0 contacts.

To export notes from GoldMine 4.0, follow these steps:

1. Launch GoldMine 4.0.
2. Choose **Export Records** from the **Tools** menu.
3. Select **Export to a new file** and **ASCII file**, and click **Next**.
4. In the list of GoldMine Fields on the left side of the dialog, select the `company`, `lastname`, and `notes` fields, and click **Add Field**. Then click **Next**.
5. Choose the location for the export file, and click **Next**.
6. Select **No** when asked if you want to save these settings, and click **Next**.
7. Click **Finish**.
8. After the export finishes, locate the exported file and change its file extension to .csv.
9. Open the file.
10. Add a header column by right-clicking on the first row and choosing **Insert**.

11. In column A, enter `Company`.
12. In column B, enter `Last Name`.
13. In column C, enter `Note`.
14. If necessary, clean up the file prior to importing it. Common problems include notes that have been broken between columns (this occurs when notes contain quotation marks).

SEE ALSO:

Field Mapping for Other Data Sources and Organization Import

Create Export Files for Import Wizards

Exporting from GoldMine 5.0

GoldMine 5.0 allows you to export contact data in a text format that can be imported. Additionally, you can export GoldMine 5.0 notes for import into Professional, Enterprise, Unlimited, Performance, and Developer Edition organizations.

- Exporting Contacts from GoldMine 5.0
- Exporting Notes from GoldMine 5.0

Exporting Contacts from GoldMine 5.0

To export contact data from GoldMine 5.0, follow these steps:

1. Launch GoldMine 5.0.
2. Choose **Tools** > **Import/Export Wizard** > **Export Contact Records**.
3. Select **Export to a new file** and **ASCII file**, and click **Next**.
4. Select **ALL Contact Records!** in the drop-down list, and click **Next**.
5. In the list of GoldMine Fields on the left side of the dialog, select the fields you want to export, and click **Add Field**. We recommend you select all fields, except the `notes` field. See Exporting Notes from GoldMine 5.0 on page 354 for information on how to export notes.
6. Click **Next**.
7. Choose the location for the export file, select the **Export GoldMine field names...** checkbox, and then click **Next**.
8. Select **No** when asked if you want to save these settings, and click **Next**.
9. Click **Finish**.
10. After the export finishes, locate the exported file and change its file extension from .txt to .csv. The file is now ready for import into Salesforce.

Exporting Notes from GoldMine 5.0

Before importing your GoldMine 5.0 notes into Salesforce, you must import your GoldMine 5.0 contacts.

To export notes from GoldMine 5.0, follow these steps:

1. Launch GoldMine 5.0.
2. Choose **Tools** > **Import/Export Wizard** > **Export Contact Records**.
3. Select **Export to a new file** and **ASCII file**, and click **Next**.
4. Select **ALL Contact Records!** in the drop-down list, and click **Next**.

5. In the list of GoldMine Fields on the left side of the dialog, select the `company`, `lastname`, and `notes` fields, and click **Add Field**. Then click **Next**.
6. Choose the location for the export file, select the **Export GoldMine field names...** checkbox, and then click **Next**.
7. Select **No** when asked if you want to save these settings, and click **Next**.
8. Click **Finish**.
9. After the export finishes, locate the exported file and change its file extension from .txt to .csv.
10. Open the file.
11. If necessary, clean up the file prior to importing it. Common problems include notes that have been broken between columns (this occurs when notes contain quotation marks).

SEE ALSO:

Field Mapping for Other Data Sources and Organization Import

Create Export Files for Import Wizards

Exporting from Palm Desktop

The Palm Desktop allows you to export your Address Book contacts in a CSV (comma-separated values) format which can then be imported.

1. Open the Address Book in the Palm Desktop. If you only want to export specific contacts, select those records.
2. Choose **Export** from the **File** menu.
3. In the "Export To File" dialog, enter a name for the file and choose a folder for it. In the **Export as** drop-down list, choose "Comma Separated (*.csv;*.txt)". Select the range of records to export - either **All** or **Currently selected records**.

   Note: If commas are not appropriate for your locale, use a tab or other delimiter.

4. Click **Export**.
5. In the "Specify Export Fields" dialog box, select the Address Book fields you want to export, and click **OK**.

SEE ALSO:

Field Mapping for Other Data Sources and Organization Import

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 are not appropriate for your locale, use a tab or other delimiter.

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, contact, custom object, lead, or solution reports from Salesforce to create an import file for the import wizards. You must include the `Account 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.

To create an import file with these ID fields, you first need to export the data from Salesforce.

1. Run an account, contact, custom object, lead, or solution report in Salesforce, include the respective ID field, and export it to Excel.
2. If you are exporting both leads and contacts to be targeted in a campaign:
   a. In Excel, combine the exported reports into one CSV (comma-separated values) file. Make sure all of the ID field values are in the same column.

      Note: If commas are not appropriate for your locale, use a tab or other delimiter.

   b. Rename the `Lead ID/Contact ID` column to `Record Id`.
   c. Add a column entitled `Status`, and enter the campaign member status for each contact or lead.

Note: Remember that Salesforce record IDs are case-sensitive and should never be changed manually in your import file.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

SEE ALSO:

Create Export Files for Import Wizards

Preparing Your Data for Import

After exporting your data from Salesforce or your existing application, prepare your data before importing it.

Note: If your data has information in fields that do not match any of the standard fields, your administrator can create custom fields for that data prior to import.

You must include universally required fields in your import files or the import will fail.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Preparing Contacts

When importing from ACT! or Outlook, the Import My Contacts wizard automatically maps fields from ACT! and Outlook to Salesforce.

When importing from other data sources, 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 363.

Preparing Person Accounts

When importing person accounts, use the field labels in Salesforce as the column labels in your import file.

Preparing Organization's Business Accounts and Contacts

When importing business accounts and contacts for your organization, 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 363.

Preparing Organization's Leads

When importing general leads or leads for campaigns, use the import file labels specified in Field Mapping for Importing Leads on page 367.

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 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 organization 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, then the potentially malicious HTML is either automatically removed or transformed into text for users who view the HTML solution. Note that users will not be able to 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 automatically removed when saved in HTML solutions. Furthermore, the content of all `<script>` and `<iframe>` tags, as well as all JavaScript, is automatically removed when saved in HTML solutions. Additionally, Cascading Style Sheets (CSS) are not supported in HTML solutions.

The following HTML tags are allowed in HTML solutions imported into Salesforce:

`<a>`	`<dt>`	`<q>`
`<abbr>`	`<em>`	`<samp>`
`<acronym>`	`<font>`	`<small>`
`<address>`	`<h1>`	`<span>`
`<b>`	`<h2>`	`<strike>`
`<bdo>`	`<h3>`	`<strong>`
`<big>`	`<h4>`	`<sub>`
`<blockquote>`	`<h5>`	`<sup>`
` `	`<h6>`	`<table>`
`<caption>`	`<hr>`	`<tbody>`
`<cite>`	`<i>`	`<td>`
`<code>`	`<img>`	`<tfoot>`
`<col>`	`<ins>`	`<th>`

<colgroup>	<kbd>	<thead>
<dd>		<tr>
<del>		<tt>
<dfn>	<p>	
	<pre>	<var>
<dl>		

Within the above tags, you can include the following attributes:

alt	face	size
background	height	src
border	href	style
class	name	target
colspan	rowspan	width

The above attributes which can include a URL are limited to URLs that begin with the following:

- http:
- https:
- file:
- ftp:
- mailto:
- #
- / for relative links

SEE ALSO:

Default Field Mapping for ACT!

Default Field Mapping for Outlook

Create Export Files for Import Wizards

Default Field Mapping for ACT!

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.

EDITIONS

Available in: Salesforce Classic

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

ACT! Field	Import Field
Address 1	Contact: Mailing Address and Account: Billing Address
Address 2	Contact: Mailing Address and Account: Billing Address
Address 3	Contact: Mailing Address and Account: Billing Address
Alt Phone	Contact: Other Phone
Alt Phone Ext.	Contact: Other Phone Ext.
Assistant	Contact: Assistant's Name
Asst. Phone	Contact: Asst. Phone
Asst. Phone Ext.	Contact: Asst. Phone Ext.
City	Contact: Mailing City and Account: Billing City
Company	Account: Name
Contact	Contact: Full Name
Country	Contact: Mailing Country and Account: Billing Country
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

ACT! Field	Import Field
Home Phone	Contact: Home Phone
Home State	Contact: Other State
Home Zip	Contact: Other Postal Code
ID/Status	Account: Type
Last Name	Contact: Last Name
Mobile Phone	Contact: Mobile Phone
Note	Does not import
Phone	Contact: Phone and Account: Phone
Phone Ext.	Contact: Business Phone Ext.
Referred By	Contact: Lead Source
Revenue	Account: Annual Revenue
State	Contact: Mailing State and Account: Billing State
Ticker Symbol	Account: Ticker Symbol
Title	Contact: Title
Web Site	Account: Website
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

ACT! Field	Import Field
	contact or account note; separate notes are not created for each ACT! field.)

SEE ALSO:

- Exporting from ACT!
- Preparing 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`

Outlook Field	Import Field
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
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,	Contact: Note or Account: Note (In Professional, Enterprise, Unlimited, Performance, and Developer Edition organizations, you specify which fields import into a single

Outlook Field	Import Field
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 or account note; separate notes are not created for each Outlook field.)

SEE ALSO:

Exporting from Outlook

Preparing Your Data for Import

Field Mapping for Other Data Sources and Organization Import

If you are importing accounts and contacts for an organization, or importing individual data from sources other than Outlook or ACT!, the Import Wizards map the fields as correctly as possible. You must fine-tune the mapping before completing the import. Before importing your data, Salesforce recommends that you use Excel to label the columns in your import file with the labels listed below. Field length limits for each object are listed in the Salesforce Field Reference Guide.

Note: The default mappings listed below are offered as a guide for importing; they do not ensure 100% accuracy in mapping your data. **You must fine-tune the mapping in the Import Wizards.** Remember that you can map the same field multiple times if necessary—for example, for the account and contact address fields.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Organization import not available in: **Personal** Edition, **Database.com**

Common Fields for Contacts and Accounts

Label for Your Import File	Salesforce Field
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 350.)	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 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

Contact Fields

Label for Your Import File	Salesforce Field
Mailing State	Contact: Mailing State/Province
Mailing Street 1	Contact: Mailing Address
Mailing Street 2	Contact: Mailing Address
Mailing Street 3	Contact: Mailing Address
Mobile Phone	Contact: Mobile
Mobile Phone Ext.	Appended to Contact: Mobile
Other City	Contact: Other City
Other Country	Contact: Other Country
Other Phone	Contact: Other Phone
Other Phone Ext.	Appended to Contact: Other Phone
Other Postal Code	Contact: Other Address Zip/Postal Code
Other State	Contact: Other State/Province
Other Street 1	Contact: Other Address
Other Street 2	Contact: Other Address
Other Street 3	Contact: Other Address
Reports To (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 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	Account: Parent Account

Account Fields	
Label for Your Import File	**Salesforce Field**
(Note: If the import wizard cannot find an account that matches the parent account name, it will create a new account using this value as the `Account Name`.)	
`Parent Account Site` (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`
`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:

Preparing Your Data for Import

Field Mapping for Importing Leads

When you import leads, the Data Import Wizard and the campaign Import Leads wizard map the fields in your import file as correctly as possible, but you must fine-tune the mapping before completing the import. Prior to importing your leads, it is recommended that you use Excel to label the columns in your lead import file with the labels listed in the following table.

Note: The following default mappings are offered as a guide. They don't ensure 100% accuracy in mapping your data, so you must fine-tune the mapping in the Import Wizard.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Label for Your Import File	Salesforce Lead Field
`Annual Revenue`	`Annual Revenue`
`City`	`City`
`Company`	`Company`
`Country`	`Country`
`Currency ISO Code` (Note: You can use this field only for organizations that use multiple currencies; see Importing Multiple Currencies on page 350.)	`Lead Currency`
`Description`	`Description`
`Email` (The import wizard verifies this is a valid email address in the form: 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: 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.)	`Lead Division`
`Lead ID` (Note: Record IDs are case-sensitive and should not be changed.)	`Lead ID`
`Lead Source` (Note: You do not need to specify this field if you choose to assign the same `Lead Source` to all leads on the first page of the import wizard.)	`Lead Source`

Label for Your Import File	Salesforce Lead Field
`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 assigning ownership via a lead assignment rule. In addition, when importing records by Salesforce record ID, this field is ignored.)	`Lead Owner`
`Salutation`	Added to beginning of `First Name`
`State`	`State`
`Status` (For campaign Import Leads wizard only.)	`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 choose to 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:

Preparing Your Data for Import

Importing My Contacts from Outlook or ACT!

Individual users can import up to 500 contacts and business accounts from Outlook or ACT! with the Import My Contacts wizard.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the unified Data Import Wizard. (Individual import wizards open in small pop-up windows, while the unified wizard opens in a full browser with dataimporter.app at the end of the URL.) To start using the unified wizard, from Setup, enter *Data Import Wizard* in the Quick Find box, then select **Data Import Wizard**. (The options you see depend on your permissions.)

Before starting the Import My Contacts wizard, create an export file and correctly prepare your data. If you are not importing from ACT! or Outlook, use the instructions in Import My Contacts from Other Sources.

Tip: You can only import data into fields that you can edit.

1. From your personal settings, enter *Import* in the Quick Find box, select **Import My Accounts & Contacts**, and click **Start the Import Wizard!**. Alternatively, click the **Import My Accounts & Contacts** link in the Tools area of the account home page.

   Labels for contacts and business accounts may have been renamed by your administrator, in which case the "Import My..." links may have customized text.

2. Specify whether your data came from Act! or Outlook. Click **Next**.
3. Click **Choose File** to upload your file.

   Note: Import a small test file to make sure that you've prepared your import file correctly.

4. Optionally, click **Customize Mappings** to verify field mappings.
5. Click **Import Now!** to complete your import.

You can also view the following video playlist to get more information: Importing Your Accounts and Contacts.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To import your contacts and accounts:

- "Import Personal Contacts"

IN THIS SECTION:

Import My Contacts from Other Sources

With the Import My Contacts wizard, you can import up to 500 contacts and associated business accounts from almost any source.

Data Import Wizard

The Data Import Wizard makes it easy to import data for many standard Salesforce objects, including accounts, contacts, leads, solutions, person accounts, and articles. The wizard also lets you import data for custom objects. With the wizard, you can import up to 50,000 records at a time.

Data Import Wizard FAQ

SEE ALSO:

Data Import Wizard
What Is Imported for Custom Objects?
Create Export Files for Import Wizards
Exporting from ACT!
Exporting from Outlook
Preparing Your Data for Import
Field Mapping for Other Data Sources and Organization Import
Importing Overview

Import My Contacts from Other Sources

With the Import My Contacts wizard, you can import up to 500 contacts and associated business accounts from almost any source.

Before starting the Import My Contacts wizard, create an export file and correctly prepare your data. If you're importing from ACT! or Outlook, see Importing My Contacts from Outlook or ACT!.

Your export file format must be a comma delimited text file (.csv).

Tip: You can import data only into fields that you can edit.

1. From Setup, enter *Import* in the Quick Find box, select **Import My Accounts & Contacts**, and then click **Start the Import Process**. Alternatively, click the **Import My Accounts & Contacts** link in the Tools area of the account home page.

   Your administrator can rename labels for contacts and business accounts, in which case, the "Import My..." links can have customized text.

2. Click **Next**.
3. To upload your file, click **Choose File**.

   Note: To make sure that you've prepared your import file correctly, import a small test file.

4. If necessary, change the default character encoding setting.
5. Choose whether duplicates will be identified by email address or name, and then click **Next**.
6. To ensure that contact data is entered into the correct fields, review the default mappings and correct any incorrect mappings, and then click **Next**.
   - You're automatically assigned as the owner for any contacts or business accounts that you import, so mapping to a Record Owner field isn't necessary.
   - To overwrite your existing business account information with imported data, select **Overwrite existing account values**. If imported data fields are blank, existing data isn't deleted.
7. If some fields don't map, and your organization is a Professional, Enterprise, Unlimited, Performance, or Developer Edition organization, you can choose not to import unmapped fields or choose to have data from unmapped fields imported as a Note for the contact or business account. All unmapped imported data for a record is included in a single note.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To import your contacts:

- "Read", "Create", "Edit" and "Delete" on contacts

  AND

  "Modify All Data" on contacts

8. To complete your import, click **Import Now!**.

View this video playlist for more information: Importing Your Accounts and Contacts.

SEE ALSO:

- Data Import Wizard
- What Is Imported for Custom Objects?
- Create Export Files for Import Wizards
- Preparing Your Data for Import
- Field Mapping for Other Data Sources and Organization Import
- Importing Overview

Data Import Wizard

USER PERMISSIONS

To import accounts and contacts:	"Import Personal Contacts"
To import leads:	"Import Leads"
To import solutions:	"Import Solutions"
To import custom objects:	"Import Custom Objects"
To import your organization's person accounts:	"Modify All Data"
To import articles:	"Modify All Data"

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

The Data Import Wizard makes it easy to import data for many standard Salesforce objects, including accounts, contacts, leads, solutions, person accounts, and articles. The wizard also lets you import data for custom objects. With the wizard, 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

Dragging and dropping CSV files is not supported in Internet Explorer 9.

SEE ALSO:

- Import Data with the Data Import Wizard

Data Import Wizard FAQ

IN THIS SECTION:

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, and custom objects.

SEE ALSO:

Data Import Wizard FAQ

Can I do simultaneous imports?

The Data Import Wizard does not support simultaneous—or concurrent—data import jobs. You must 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 administrator, 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 administrator, and you want to know the status of an import, you'll 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

Using the Import Queue

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the unified Data Import Wizard. (Individual import wizards open in small pop-up windows, while the unified wizard opens in a full browser with dataimporter.app at the end of the URL.) To start using the unified wizard, from Setup, enter *Data Import Wizard* in the Quick Find box, then select **Data Import Wizard**. (The options you see depend on your permissions.)

Administrators can check the Import Queue to view details about an import or to cancel an organization import. Import details are removed from the queue three days after completion.

1. From Setup, enter *Imports* in the Quick Find box, then select **Imports**.
2. Select the file name of the import file to see the Import Queue Detail page for that file.

If you want to cancel an import, and the import has not started processing, click **Del**. You cannot cancel an import after it has started processing.

The possible values of the Status column are listed below:

Status	Description
Aborted	The import did not complete successfully. The error details are emailed to the user who performed the import. Aborted imports can be retried within three days, but, if multiple retry attempts are made, the import cannot remain in the queue for more than 30 days from the original import attempt.
Completed	The import completed successfully without errors.
Error	The import was processed and errors were encountered. The error details are emailed to the user who performed the import. The user can fix the errors, and then attempt the import again.
Pending	The import is in the queue but has not started processing yet.
Processing	The import is in the queue and is currently being processed.

SEE ALSO:

Data Import Wizard

Importing Overview

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

User Permissions Needed

To use the Import Queue:

- "Modify All Data"

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 Performing Mass Deletes on page 387.

SEE ALSO:

- Data Import Wizard
- Importing Overview

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"

Data Loader

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 are not appropriate for your locale, use a tab or other delimiter.

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 XP, Windows 7, and Mac OS X

To get started, see the following topics:

- When to Use Data Loader
- Installing Data Loader

Note: In previous versions, Data Loader has been known as "AppExchange Data Loader" and "Sforce Data Loader."

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 Importing Overview on page 342.

Install and Configure Data Loader

Considerations for Installing 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:
- The appropriate user permission for the operation you are doing, for example, "Create" on accounts to insert new accounts

System Requirements for Windows

To use Data Loader for Windows, you need:

- Microsoft® Windows® 7 or Windows XP
- 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 Mac OS

To use Data Loader for Mac, you need:

- Mac® OS X
- 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 391.

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

The latest version of Data Loader supports Web Server OAuth Authentication for both Windows and Mac, which provides an extra layer of security compliance. See OAuth Authentication for more information.

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.

Configure Data Loader

Use the Settings menu to change the default operation settings of Data Loader.

1. Open the Data Loader.
2. Choose **Settings** > **Settings**.
3. Edit the fields as desired:

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 value is 200. We recommend a value between 50 and 100. The maximum value is 10,000 if the `Use Bulk API` option is selected.
`Insert null values`	Select this option to insert blank mapped values as `null` values during data operations. Note that when you are updating records, this option instructs Data Loader to overwrite any 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`.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Field	Description
`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 may want to disable compression if you need to debug 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`.
`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.
`Use Bulk API`	Select this option to use the Bulk API to insert, update, upsert, delete, and hard delete records. The Bulk API is optimized to load or delete a large number of records asynchronously. It's faster than the default SOAP-based API due to parallel processing and fewer network round-trips.

Field	Description
	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`	Select this option to use serial instead of parallel processing for Bulk API. Processing in parallel can cause database contention. When this is severe, the load may fail. Using serial mode guarantees that batches are processed one at a time. Note that using this option may significantly increase the processing time for a load. This option is only available if the `Use Bulk API` option is selected.
`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

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 378.

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

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 this is severe, the load may fail. Using serial mode guarantees that batches are processed one at a time. Note that using this option may significantly 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

Use Data Loader

Data Types Supported by Data Loader

EDITIONS

Available in: Salesforce Classic

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 387 and Upload Content with the Data Loader on page 388.

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.

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*.

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

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 Reviewing Data Loader Output Files on page 389.

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

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 385.

EDITIONS

Available in: Salesforce Classic

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

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

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

The insert, update, upsert, delete, and hard delete wizards in Data Loader allow you to add new records, modify existing records, or delete existing records. Note that "upsert" is a combination of inserting and updating. 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, then the record is created as new. When you hard delete records, the deleted records are not stored in the Recycle Bin and become immediately eligible for deletion. For more information, see Configure Data Loader on page 378.

1. Open the Data Loader.
2. Click **Insert**, **Update**, **Upsert**, **Delete** or **Hard Delete**. 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 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, check `Show all objects` to see a complete list of the objects that you can access. The objects are listed by localized label name, with developer name noted in parentheses. For object descriptions, see the *Object Reference for Salesforce and Force.com*.

5. Click **Browse...** to select your CSV file. For example, if you are inserting Account records, you could specify a CSV file named `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:
   a. Your CSV file must contain a column of ID values for matching against existing records. The column may be either an external ID (a custom field with the "External ID" attribute), or `Id` (the Salesforce record ID). From the drop-down list, select which field to use for matching. If the object has no external ID fields, `Id` is automatically 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 drop-down list. If you make no selection here, 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. Click **Choose an Existing Map** to select an existing field mapping, or click **Create or Edit a Map** to create a new map or modify an existing map. For more details and an example of usage, see Define Data Loader Field Mappings on page 385.
9. Click **Next**.
10. For every operation, the Data Loader generates two unique CSV log files; one file name starts with "success," while the other starts with "error." Click **Browse...** to specify a directory for these files.
11. Click **Finish** to perform the operation, and then click **Yes** to confirm.
12. As the operation proceeds, a progress information window reports the status of the data movement.
13. After the operation completes, a confirmation window summarizes your results. Click **View Successes** to view your success file, click **View Errors** to open your errors file, or click **OK** to close. For more information, see Reviewing Data Loader Output Files on page 389.

Tip:

- If you are updating or deleting large amounts of data, review Perform Mass Updates and Performing Mass Deletes for tips and best practices.
- There is a five-minute limit to process 100 records when the Bulk API is enabled. Also, 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 failed, some records could have completed successfully, so you must 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 385.
5. After the operation, review your success and error log files. See Reviewing Data Loader Output Files on page 389.
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

Performing 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 383.) 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 385.
4. After the operation, review your success and error log files. See Reviewing Data Loader Output Files on page 389.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

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 Exporting Backup Data on page 425.

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 385. 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

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/36.0/debugshell.html`. Enter the *instanceName*, such as *na1*, 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 385). All documents and links are available in the specified library.

Reviewing Data Loader Output Files

After every import or export, Data Loader generates two CSV output files that contain the results of the operation. One file name starts with "success," while the other starts with "error." During every export, Data Loader saves the extracted data to a CSV file that you specify in the wizard. Data Loader has a built-in CSV file viewer with which you can open and view these files.

EDITIONS

Available in: Salesforce Classic

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

To view output files from a Data Loader operation:

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 1000.
3. To view a CSV file of your choice, click **Open CSV**. To view the last success file, click **Open Success**. To view the last error file, click **Open Error**. The CSV file opens in a new window.
4. Optionally, click **Open in External Program** to open the file in the associated external program, such as Microsoft® Office Excel.

   The "success" file contains all of the records that were successfully loaded. In this file, there's a column for the newly generated record IDs. The "error" file contains all of the records that were rejected from the load operation. In this file, there's a column that describes why the load failed.
5. Click **Close** to return to the CSV Chooser window, and then click **OK** to exit the window.

Note: To generate success files when exporting data, select the `Generate status files for exports` setting. For more information, see Configure Data Loader on page 378.

View the Data Loader Log File

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`*.

EDITIONS

Available in: Salesforce Classic

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

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.

Run Batch Processes (Windows Only)

Batch Mode

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

EDITIONS

Available in: Salesforce Classic

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

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 392.

Installed Directories and Files

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:

EDITIONS

Available in: Salesforce Classic

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

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 392.

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

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:

EDITIONS

Available in: Salesforce Classic

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

- `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

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 392.

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 391.

Data Loader Command-Line Interface

Note: The Data Loader command-line interface is supported for Windows only.

EDITIONS

Available in: Salesforce Classic

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 Introduction on page 409 and Encrypt from the Command Line on page 391. 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 408.

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 391.

Configure Batch Processes

Note: The Data Loader command-line interface is supported for Windows only.

EDITIONS

Available in: Salesforce Classic

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

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 394.

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 graphical user interface at **Settings** > **Settings**.

Tip: A sample `process-conf.xml` file can be found in the `\samples` directory that's installed with Data Loader.

EDITIONS

Available in: Salesforce Classic

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

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`

Parameter Name	Data Type	Equivalent Option in Settings Dialog	Description
			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`
`dataAccess.writeBatchSize`	integer	N/A	
`process.enableExtractStatusOutput`	boolean	`Generate status files for exports`	Select this option to generate success and error files when exporting data. Sample value: `true`
			When running Data Loader in batch mode, you can disable the generation of output files such as `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.enableLastRunOutput`	boolean	N/A	
`process.encryptionKeyFile`	string (file name)	N/A	Name of the file that contains the encryption key. See Encrypt from the Command Line on page 391. Sample value: `c:\dataloader\conf\my.key`
			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 382. Format must be `yyyy-MM-ddTHH:mm:ss.SSS+/-HHmm`. For example: 2006-04-13T13:50:32.423-0700
`process.initialLastRunDate`	date	N/A	

Parameter Name	Data Type	Equivalent Option in Settings Dialog	Description
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 407. Sample value: c:\dataloader\conf\accountExtractMap.sdl
process.operation	string	N/A	The operation to perform. See Data Loader Command-Line Operations on page 402. 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 395. Sample value: c:\dataloader\status\myProcessSuccesses.csv

Parameter Name	Data Type	Equivalent Option in Settings Dialog	Description
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
sfdc.bulkApiSerialMode	boolean	Enable serial mode for Bulk API	Select this option to use serial instead of parallel processing for Bulk API. Processing in parallel can cause database contention. When this is severe, the load may fail. Using serial mode guarantees that batches are processed one at a time. Note that using this option may significantly 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

Parameter Name	Data Type	Equivalent Option in Settings Dialog	Description
			alternate location in `sfdc.debugMessagesFile`. Sample value: `false`
`sfdc.debugMessagesFile`	string (file name)	N/A	See `process.enableExtractStatusOutput` on page 395. 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 399 and `sfdc.minRetrySleepSecs` on page 399. 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 data into a sandbox, change the URL to `https://test.salesforce.com`. Sample production value: `https://login.salesforce.com/services/Soap/u/36.0`
`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`

Parameter Name	Data Type	Equivalent Option in Settings Dialog	Description
`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. Note that when you are updating records, this option instructs Data Loader to overwrite any 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 value is 200. 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 398. Sample value: `3`
`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 398. Sample value: `2`
`sfdc.noCompression`	boolean	`Compression`	Compression enhances the performance of Data Loader and is turned on by default. You may want to disable compression if you need to debug 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 391. Sample value: `4285b36161c65a22`

Parameter Name	Data Type	Equivalent Option in Settings Dialog	Description
`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 391. 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`
`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`.

Parameter Name	Data Type	Equivalent Option in Settings Dialog	Description
			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. Sample value: `true`
`sfdc.useBulkApi`	boolean	`Use Bulk API`	Select this option to use the Bulk API to insert, update, upsert, delete, and hard delete records. The Bulk API is optimized to load or delete a large number of 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.

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.

EDITIONS

Available in: Salesforce Classic

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

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

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

Note: The Data Loader command-line interface is supported for Windows only.

EDITIONS

Available in: Salesforce Classic

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

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

Note: The Data Loader command-line interface is supported for Windows only.

EDITIONS

Available in: Salesforce Classic

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

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

Note: The Data Loader command-line interface is supported for Windows only.

EDITIONS

Available in: Salesforce Classic

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

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

Note: The Data Loader command-line interface is supported for Windows only.

EDITIONS

Available in: Salesforce Classic

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

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.

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`.

EDITIONS

Available in: Salesforce Classic

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

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.

Command-Line Quick Start (Windows Only)

Data Loader 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

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

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

Step One: Create the Encryption Key

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 need to provide the information that you would normally enter in the user interface by using 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 clicking **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.

EDITIONS

Available in: Salesforce Classic

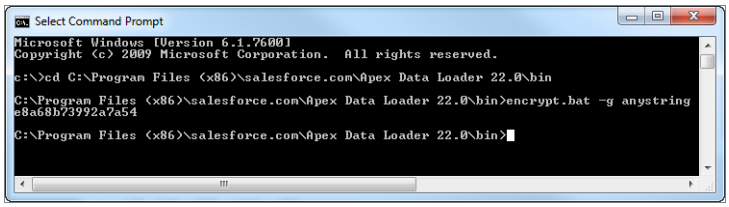
Available in: **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

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>
   ```



   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 is used to encrypt passwords, but data that you transmit using Data Loader is not encrypted.

SEE ALSO:

Step Two: Create the Encrypted Password

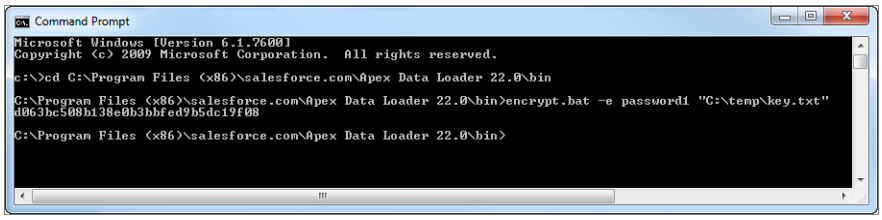
Step Two: Create the Encrypted Password

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"
   ```



EDITIONS

Available in: Salesforce Classic

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

2. Copy the encrypted password that is generated by the command. You use this value in a later step.

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.

EDITIONS

Available in: Salesforce Classic

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

The field mapping file associates data sources with destinations. This is a text file, typically with an `.sdl` file extension.

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**.

SEE ALSO:

Step Four: Create the Configuration File

Step Four: Create the Configuration File

Note: The Data Loader command-line interface is supported for Windows only.

EDITIONS

Available in: Salesforce Classic

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

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 394.
   - `sfdc.endpoint`—Enter the URL of the Salesforce instance for your organization; for example, `https://na1.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

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 Reviewing Data Loader Output Files on page 389.

Data Loader Third-Party Licenses

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

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Note: Salesforce is not responsible for the availability or content of third-party websites.

Importing FAQ

General Importing Questions

- Can I mass upload data into Salesforce?
- Should I sync Outlook or use import wizards to upload my data into Salesforce?
- Who in my organization can use the import wizards?
- What permissions do I need to import records?
- What file formats can the import wizards handle?
- What data can I import?
- Are there size restrictions on my import data?
- Why can't I log in to Data Loader?
- Why isn't Data Loader importing special characters?

EDITIONS

Available in: Salesforce Classic

Available in all editions

SEE ALSO:

Importing Campaign Members

Can I mass upload data into Salesforce?

Group, Professional, Performance, Unlimited, Enterprise, and Developer editions have the Data Import Wizard for accounts, contacts, leads, and custom objects that allow you to mass import data. To access them, from Setup, click **Data Management**. In addition, Performance, Unlimited, Enterprise, and Developer editions have API access to use database mass upload tools like Data Loader.

Should I sync Outlook or use import wizards to upload my data into Salesforce?

Use the following information to determine how to upload data into your Salesforce organization.

- 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, we recommend that you use Exchange Sync or Salesforce for Outlook to initially sync your data and for all subsequent updates.
- To upload custom objects, leads, 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 Exchange 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**.
- To upload person accounts, use the Import My Person Accounts wizard.

Note: When you import person accounts, the following limitations apply.

- The unified Data Import Wizard doesn't support person accounts.
- You can't upload person accounts by using 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 372.

Who in my organization can use the import wizards?

All users in your organization can use the Import My Contacts wizard. In Enterprise, Unlimited, Performance, or Developer Edition organizations with person accounts enabled, all users can use the Import My Person Accounts wizard.

Only an administrator can use the organization-wide Data Import Wizard to import accounts, contacts, leads, solutions, or custom objects for multiple users at one time. In Personal Edition, the Data Import Wizard isn't available. In Contact Manager Edition, leads and solutions in the Data Import Wizard aren't available. In Group Edition, solutions in the Data Import Wizard isn't available.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the unified Data Import Wizard. (Individual import wizards open in small pop-up windows, while the unified wizard opens in a full browser with dataimporter.app at the end of the URL.) To start using the unified wizard, 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

To import records with the Data Loader, you need "Create" permission on the record you want to import.

Import Wizard for Records You Own

Records being imported	Access needed
My Contacts	"Import Personal Contacts"
My Person Accounts	"Create" on accounts AND "Read" on contacts AND "Import Personal Contacts" AND At least one person account record type available from your profile or permission sets

Import Wizard for Records Owned By Other Users

Records being imported	Access needed
My Organization's Accounts and Contacts	"Modify All Data" OR "Import Personal Contacts"

Records being imported	Access needed
My Organization's Person Accounts	"Modify All Data" OR "Import Personal Contacts"
My Organization's Leads	"Read", "Create", and "Edit" on leads AND "Import Leads"
My Organization's Solutions	"Import Solutions"
My Organization's Custom Objects	"Import Custom Objects"

Import Wizard for Campaign Members

Records being imported	Access needed
New Campaign Members (Data Import Wizard)	"Edit" on campaigns AND `Marketing User` checked in your user information AND "Import Leads"
Updated Campaign Members (Campaign Update Wizard)	"Edit" on campaigns AND "Import Leads" AND "Read" on contacts AND `Marketing User` checked in your user information

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the unified Data Import Wizard. (Individual import wizards open in small pop-up windows, while the unified wizard opens in a full browser with dataimporter.app at the end of the URL.) To start using the unified wizard, 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 are not appropriate for your locale, use a tab or other delimiter.

What data can I import?

You can use import wizards to import the following records:

Contacts and business accounts
Use the Import My Contacts wizard and the Data Import Wizard to import contacts and business accounts.

In Professional, Enterprise, Unlimited, Performance, and Developer Edition organizations, you can also import contact and business account notes.

Person accounts
In Enterprise, Unlimited, Performance, and Developer Edition organizations, use the Import My Person Accounts wizard to import person accounts that you own. Administrators can use the Import My Organization's Person Accounts wizard to import person accounts for multiple users.

Leads
In Professional, Enterprise, Unlimited, Performance, and Developer Edition organizations, use the Data Import Wizard to import leads.

Solutions
In Professional, Enterprise, Unlimited, Performance, and Developer Edition organizations, use the Data Import Wizard to import solutions.

Custom objects
In Contact Manager, Group, Professional, Enterprise, Unlimited, Performance, and Developer Edition organizations, use the Data Import Wizard to import custom objects.

You can import values into a field only if you have read and edit access. Field access is determined by user permissions, page layout assignments, and field-level security settings.

Import wizards for other records are not available.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the unified Data Import Wizard. (Individual import wizards open in small pop-up windows, while the unified wizard opens in a full browser with dataimporter.app at the end of the URL.) To start using the unified wizard, from Setup, enter `Data Import Wizard` in the `Quick Find` box, then select **Data Import Wizard**. (The options you see depend on your permissions.)

Are there size restrictions on my import data?

Yes. Your import file cannot exceed 100MB in size, and each record in the file cannot be bigger than 400KB. In addition, each imported note and each imported description cannot exceed 32KB. Descriptions longer than 32KB are truncated.

In addition to the import file limits, your import is also subject to the overall storage limits for your organization. Note that the size of your import file does not directly correlate to the storage space needed for those records. For example, an import file of 50MB in size may not create 50MB of data in Salesforce.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the unified Data Import Wizard. (Individual import wizards open in small pop-up windows, while the unified wizard opens in a full browser with dataimporter.app at the end of the URL.) To start using the unified wizard, 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?

If you're having trouble logging in to Data Loader, try the following solutions.

- Add a security key 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://instance_name.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.

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:

Importing Overview

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. Field access is determined by user permissions, page layout assignments, and field-level security settings.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the unified Data Import Wizard. (Individual import wizards open in small pop-up windows, while the unified wizard opens in a full browser with dataimporter.app at the end of the URL.) To start using the unified wizard, 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 unified Data Import Wizard. (Individual import wizards open in small pop-up windows, while the unified wizard opens in a full browser with dataimporter.app at the end of the URL.) To start using the unified wizard, 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?

Your administrator can from Setup, 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.

For organization imports that have not begun processing, you can cancel an import in the Import Queue. From Setup, enter *Imports* in the Quick Find box, then select **Imports**. The import queue is not accessible to Personal Edition organizations.

How do I update records using the Data Import Wizard?

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.

To Update Leads

1. From Setup, enter *Data Import Wizard* in the Quick Find box, select **Data Import Wizard**, then click **Launch Wizard!**.
2. Click **Leads**.
3. Click **Update existing records**.
4. Under Matching Type, choose **Salesforce.com ID**. Click **Next**.
5. Select **Overwrite existing lead values**.
6. Map the Lead ID field to the Lead ID column in your local file, as well as all other fields.
7. Review, and click **Import Now!**.

To Update Accounts or Contacts

1. From Setup, enter *Data Import Wizard* in the Quick Find box, select **Data Import Wizard**, then click **Launch Wizard!**.
2. Click **Accounts and Contacts**.
3. Click **Update existing records**.
4. Under Contact Matching Type, choose **Salesforce.com ID**. The Account Matching Type automatically matches the Contact Matching Type. Click **Next**.
5. Map the Contact Id field to the Contact ID column in your local file, and map the other contact fields. Click **Next**.
6. Map the contact phone and address fields. Click **Next**.
7. Select **Overwrite existing account values**, map the Account Id field to the Account ID column in your local file, and map the other account fields.
8. Upload your CSV file you're importing.
9. Map the extra import fields, and click **Next**.
10. Click **Import Now!**.

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.

What does the Import Queue show me?

From Setup, enter *Imports* in the Quick Find box, then select **Imports**. The Import Queue shows all of the unprocessed files that you've submitted by using the Data Import Wizard in Setup. You can see when each file was submitted, its status, and a processing time estimate. Click **Del** to cancel an import file that has not begun processing. The import queue is not accessible to Personal Edition organizations.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the unified Data Import Wizard. (Individual import wizards open in small pop-up windows, while the unified wizard opens in a full browser with

dataimporter.app at the end of the URL.) To start using the unified wizard, 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 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 only takes a few minutes.

The administrator import wizards work asynchronously, and you will 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.

Administrators, except in Personal Edition, can also check the Import Queue to view the progress of import files. From Setup, enter *Imports* in the Quick Find box, then select **Imports**. To expedite the import process, we recommend you review the directions in Importing Overview on page 342.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the unified Data Import Wizard. (Individual import wizards open in small pop-up windows, while the unified wizard opens in a full browser with dataimporter.app at the end of the URL.) To start using the unified wizard, 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?

In order to manage the volume of imports and ensure that all users receive the highest level of performance, organization import files are accepted in "asynchronous" mode. This means that your file passes through a controlled queue and will be imported when the system can best manage the data, however your organization import will not take longer than 24 hours to complete. You will 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 organization 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 organizations 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 unified Data Import Wizard. (Individual import wizards open in small pop-up windows, while the unified wizard opens in a full browser with dataimporter.app at the end of the URL.) To start using the unified wizard, 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 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.

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.

What is an external ID?

When importing custom objects, solutions, or person accounts, you can use external IDs to prevent duplicate records from being created as a result of the import operation.

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 import wizard will detect existing records in Salesforce that have the same external ID. Note that this operation is not case-sensitive - for example, "ABC" will be matched with "abc". However, there is an exception: if the custom field has the separate "Unique" attribute and the case-sensitive option for that attribute is selected, uppercase and lowercase letters will not be considered identical.

Importing Campaign Members

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Why are there two campaign import wizards?

You can access the campaign import wizards via the **Add Members - Import File** and **Update & Add Members - Import File** links on the **Manage Members** page, which is available from any campaign detail page. The wizards are:

- **Data Import Wizard**: To access this wizard from a campaign detail page, click **Manage Members** > **Add Members - Import File** > **Leads**. Use this wizard to import leads. It imports a list of names, creates or updates leads in the system, and associates those leads with your campaign.
- **Campaign Update Wizard**: To access this wizard from a campaign detail page, click **Manage Members** > **Update & Add Members - Import File** > **Update & Add Campaign Members**. Use this wizard to update the campaign member statuses of existing leads and contacts. It imports a list of existing Salesforce contacts and leads, associates them with your campaign, and updates their response history.

How many campaign members can I import?

The number of campaign members that can be imported is determined by the following wizards:

- **Lead Import Wizard**: Import up to 50,000 leads at one time.
- **Campaign Update Wizard**: Update up to 50,000 existing contacts and leads at one time.

In addition to the record limits, your import is also subject to the overall storage limits for your organization.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the unified Data Import Wizard. (Individual import wizards open in small pop-up windows, while the unified wizard opens in a full browser with dataimporter.app at the end of the URL.) To start using the unified wizard, from Setup, enter *Data Import Wizard* in the Quick Find box, then select **Data Import Wizard**. (The options you see depend on your permissions.)

Who can import campaign members?

In order to use the Data Import Wizard to import new leads for a campaign or campaign import wizards to update the campaign history for multiple leads and contacts, users must have the Marketing User checkbox selected on their personal information. They must also have the Marketing User profile (or the "Edit" permission on campaigns and "Import Leads" permission).

What status is assigned to campaign members?

With the campaign import wizards, you can assign a campaign member status to a lead or contact in one of two ways:

- Add a Status column to your import file. Enter the status for each lead or contact on the campaign.
- Select a default status in the campaign import wizard. Any lead or contact with a blank or invalid status in your import file will automatically be assigned to the default status.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the unified Data Import Wizard. (Individual import wizards open in small pop-up windows, while the unified wizard opens in a full browser with dataimporter.app at the end of the URL.) To start using the unified wizard, 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 prepare my campaign import file?

A campaign import file can be prepared by using one of the following wizards:

- **Lead Import Wizard**: Prepare your import file of new leads using Excel.
- **Campaign Update Wizard**: Update only the member status of an existing lead or contact. Your import file must include a Status column plus a Record Id column that contains the unique Salesforce Contact ID or Lead ID values for the leads and contacts.

Important: Salesforce has replaced the individual import wizards for accounts, contacts, and other objects with the unified Data Import Wizard. (Individual import wizards open in small pop-up windows, while the unified wizard opens in a full browser with dataimporter.app at the end of the URL.) To start using the unified wizard, from Setup, enter *Data Import Wizard* in the Quick Find box, then select **Data Import Wizard**. (The options you see depend on your permissions.)

Manage Data

Exporting Backup Data

Your organization can generate backup files of your data on a weekly or monthly basis depending on your edition. You can export all your organization's data into a set of comma-separated values (CSV) files.

Note: Users with the "Weekly 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 six days (for weekly export) or 28 days (for monthly export). You can also schedule backup files to generate automatically at weekly or monthly intervals.

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.

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 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: Selecting `Include images, documents, and attachments` and `Include Chatter files and Salesforce CRM Content document versions` increases data export processing time.
4. Select `Replace carriage returns with spaces` to have spaces instead of carriage returns or line breaks in your export files. 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 organizations 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. We recommend that you select **Include all data** if you are not familiar with the terminology used for some of the types of data. Note the following:
   - Formula and roll-up summary fields are always excluded from exports.
   - If your organization uses divisions, data from all divisions is included in the export.
   - If your organization uses person accounts and you are exporting accounts, all account fields are included in the account data.
   - If your organization 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 you when it's ready. 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. Follow the link in the email or click **Data Export** to download the zip file. Zip files are deleted 48 hours after the email is sent. The 48-hour time limit doesn't include weekends, so if your download file is ready on Thursday at 4 p.m., that file isn't deleted until Monday at 4 p.m.

Note: For security purposes, Salesforce may require users to pass a CAPTCHA user verification test to export data from their organization. This simple text-entry test prevents malicious programs from accessing your organization's data. To pass the test, users must correctly type the two words displayed on the overlay into the overlay's text box field. Note that the words entered into the text box field must be separated by a space.

Tip: Any automated processes that process the export files should rely on the column headings in the CSV files, rather than the position of the columns.

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.

Viewing 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. Select the CSV file to open and Microsoft Excel launches the text import wizard.
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 are not appropriate for your locale, use a tab or other delimiter.

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. Click **OK** to close the dialog boxes.
7. Select **File** > **Save** to save the file with selected encoding.
8. Repeat these steps for each file.

Viewing 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.

Viewing 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 are not appropriate for your locale, use a tab or other delimiter.

6. Repeat these steps for each file.

Transferring Records Overview

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

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**.

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

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.
- 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 Transferring Records

Mass Transferring 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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Accounts, Service Contracts, and Leads are 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

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. Optionally, check the box in the column header to select all currently displayed items.

   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 Overview

Deleting Multiple Records and Reports

You can delete multiple reports or records at one time.

The record types you can mass-delete include cases, solutions, accounts, contacts, leads, products, and activities.

Here are some ways mass delete might be 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 organization's leads incorrectly and you want to start over.
- A user who recently left your organization had contacts that were duplicates of other users' data and you want to delete these duplicate contacts.
- Your organization 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 My Organization's 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 organization. Select the lead record type, enter "Converted equals 1" for the search criteria, then choose Search.
- You want to clean up web-generated leads that were created incorrectly, or delete accounts and contacts with whom you no longer do business.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **All** Editions

This feature is only available in **Database.com** via the API. You can only mass delete records of custom objects in **Database.com**.

USER PERMISSIONS

To mass delete data:
- "Modify All Data"

1. We strongly suggest you run a report to archive your information. You should also run a weekly export of your data; see Exporting Backup Data on page 425.
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 will be deleted along 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 other users.
6. If you're deleting products, check **Archive Products** if you also want to delete products that are on opportunities.

   Check this option to:

   - Delete products that are not on opportunities and move them to the Recycle Bin.
   - Archive products that are on opportunities. These products are not moved to the Recycle Bin and cannot be recovered.

   Leave this box unchecked to delete only those products that are not on opportunities. Selected products that are on opportunities will remain checked after the deletion to indicate they were not included in the deletion.
7. Choose **Search** to find records that match, and select the items you want to delete. Optionally, check the box in the column header to select all currently displayed items.
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:

State and Country Picklists

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.

Force.com Platform Cache

Define Partitions for Data Cached with Force.com Platform Cache

Using the Platform Cache can enable applications to run faster, by allowing them to 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 the capacity of the default partition is used up and is zero, you can't create more partitions. 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**.

SEE ALSO:

Apex Developer Guide

Request a Platform Cache Trial

Purchase Platform Cache

Request a Platform Cache Trial

If you want to test performance improvements by using Platform Cache in your own org, you can request trial cache. Enterprise, Unlimited, and Performance editions come with some cache, but often, adding more cache gives even greater performance enhancements. When your trial request is approved, you can allocate capacity to partitions and experiment with using the cache for different scenarios. Testing trial cache allows you to make an informed decision about whether to purchase more cache.

Salesforce usually approves trial cache requests in three days. When your request is approved, you receive 60 MB of trial cache space, which is active for 10 business days. 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. If you need more than 10 days to fully test cache performance, contact Salesforce.

After you request trial cache, you receive emails at the following intervals.

At activation
You have 10 business days to test the trial cache in your org. You can now allocate capacity to partitions.

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. When your trial request is approved, you receive trial cache space that doesn't expire for three to six months. 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 organization-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:

Define Partitions for Data Cached with Force.com Platform Cache

Purchase Platform Cache

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:

Define Partitions for Data Cached with Force.com Platform Cache

Request a Platform Cache Trial

Manage Duplicate Records in Salesforce

Maintaining clean and accurate data is one of the most important things you can do to help your organization get the most out of Salesforce. Use Data.com Duplicate Management to control whether and when users can create duplicate records in Salesforce; customize the logic that's used to identify duplicates; and create reports on the duplicates that users save.

Note: Duplicate Management uses Data.com technology, but does *not* require a Data.com license.

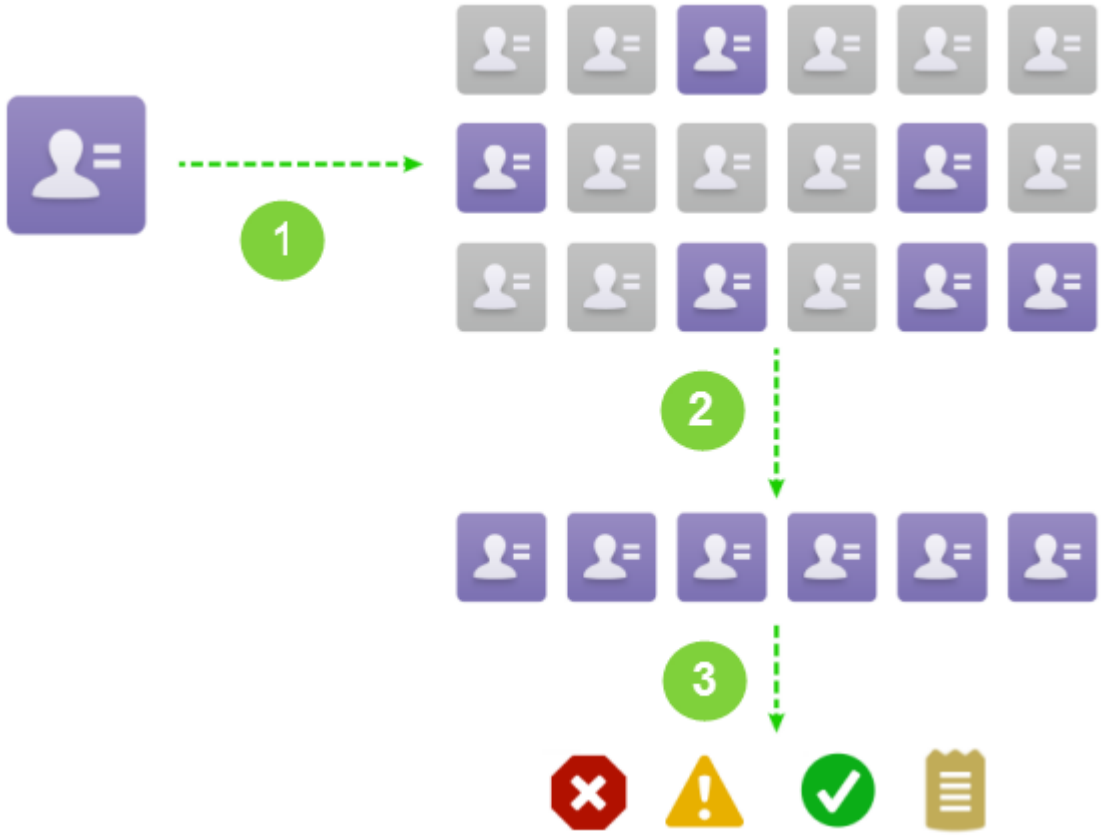
Starting in Spring '15, all new Salesforce orgs come with Duplicate Management features already set up and turned on for accounts, contacts, and leads. Other orgs must manually set up and activate Duplicate Management features. After Duplicate Management is set up, here's how it works.

- *When a user attempts to save a new record*, the record is first compared with existing Salesforce records to identify possible duplicates (1). The criteria used to compare records and identify the possible duplicates are defined by a *matching rule*. Next, a list of possible duplicates is returned (2). What happens when the record being saved is identified as a possible duplicate depends on what's defined in the *duplicate rule* (3). For example, the duplicate rule could block users from saving the possible duplicate record or allow them to save it anyway. Both the Block and Allow options include an alert, which tells users why they can't save the record and what they need to do. The Allow option includes the ability to report on the duplicate records.
- *When a user attempts to save an edited record*, the record is first checked to see if the user has changed the value of a matching rule field. If so, the duplicate management process works as described for new records. If not, no further action is taken and duplicates are not detected.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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



IN THIS SECTION:

Considerations for Using Duplicate Management

Data.com Duplicate Management includes limits for duplicate rules, matching rules, and duplicate record sets.

Duplicate Management Concepts

To configure Data.com Duplicate Management more effectively, it's important to understand some key concepts.

Set Up Duplicate Management in Salesforce

To use Data.com Duplicate Management in your organization, you need two separate rules: a duplicate rule and a matching rule. The duplicate rule tells Salesforce what action to take when duplicates are identified. The matching rule defines how records are compared to one another to identify possible duplicates.

Matching Rule Reference

Here's some additional information that will help you understand how matching rules work and how to use them.

Duplicate Rule Reference

Here's some additional information that will help you understand how duplicate rules work and how to use them.

Duplicate Management FAQs

Answers to common questions about Data.com Duplicate Management.

SEE ALSO:

Duplicate Management Concepts

Set Up Duplicate Management in Salesforce

Matching Rule Reference

Considerations for Using Duplicate Management

Data.com Duplicate Management includes limits for duplicate rules, matching rules, and duplicate record sets.

Considerations for Duplicate Rules

- Duplicate rules are available for accounts, contacts, leads, and custom objects. All other objects, including Opportunities and Person Accounts, are not currently supported.
- Duplicate rules don't run when:
  - Records are created using Quick Create.
  - Leads are converted to accounts or contacts *and* your organization doesn't have the "Use Apex Lead Convert" permission.
  - Records are restored with the **Undelete** button.
  - Records are added using Exchange Sync.
  - Records are manually merged.
  - A Self-Service user creates records and the rules include conditions based on the User object.
  - Duplicate rule conditions are set for lookup relationship fields and records with no value for these fields are saved. For example, you have a condition that specifies a duplicate rule only runs when `Campaign DOES NOT CONTAIN 'Salesforce'`. Then, if you add a record with *no value* for the `Campaign` field, the duplicate rule doesn't run.
- Sometimes, if duplicate rules are set for an alert to show when duplicates are found, users are *always* blocked from saving records and *do not* see a list of duplicates. This situation happens when:
  - Records are added using the data import tools.
  - A person account is converted to a business account (and the newly created business account matches existing business accounts).
  - Records are added or edited using Salesforce APIs.
- If you're saving multiple records at the same time and your duplicate rules are set to `Block` or `Alert`, records within the same save aren't compared to each other; they are only compared with records already in Salesforce. This behavior doesn't affect the `Report` action, and duplicate record sets include records that match other records in the same save.
- Custom picklists are not supported when they're included in a matching rule that's used in a cross-object duplicate rule.
- The customizable alert text in duplicate rules isn't supported by the Translation Workbench.
- Up to 5 active duplicate rules are allowed per object.
- Up to three matching rules are allowed per duplicate rule, and each matching rule must be of a different object.
- Starting in Spring '15, all new Salesforce orgs come with Duplicate Management features turned on for accounts, contacts, and leads. New orgs come with standard account, contact, and lead duplicate rules. Each duplicate rule is associated with a matching rule. You can deactivate these rules or create custom rules.

Considerations for Matching Rules

- Matching rules are available for accounts, contacts, leads, and custom objects. All other objects, including Opportunities and Person Accounts, are not currently supported.
- Standard and custom matching rules that use fuzzy matching methods only support Latin characters, and, if you're using international data, we recommend using the Exact matching method with your matching rules.
- If a field on an object is no longer available to your organization, it could cause matching rules with mappings to this field to be ignored and duplicate detection to be affected. Check all duplicate rule field mappings for an object if there is a change to the fields available to your organization. For example, the `Clean Status` field is only available to customers with a Data.com license. If your organization no longer has a Data.com license, this field is no longer available and matching rules with mappings to this field are ignored.
- Only 1 lookup relationship field is allowed per matching rule.
- Up to 5 active matching rules are allowed per object.
- Up to 25 total active matching rules are allowed.
- Up to 100 total matching rules are allowed (both active and inactive).
- Up to 5 matching rules can be activated or deactivated at a time.
- Matching rules that include fields with Platform Encryption do not detect duplicates. If your organization has Platform Encryption enabled, make sure that your matching rules do not include encrypted fields.

Considerations for Duplicate Record Sets

- By default, duplicate record sets are visible to only administrators, but the administrator can grant visibility to other users.
- If a lead is identified as a duplicate but converted before the duplicate record set is created, the converted lead isn't included in a duplicate set.

SEE ALSO:

Duplicate Rules

Duplicate Management Concepts

To configure Data.com Duplicate Management more effectively, it's important to understand some key concepts.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

IN THIS SECTION:

Duplicate Rules

Duplicate rules are used to control whether and when you can save duplicate records within Salesforce.

Matching Rules

Matching rules are used to identify duplicate records within Salesforce.

Duplicate Record Sets

Quickly see a list of duplicate records, grouped into duplicate sets, by clicking the Duplicate Record Sets tab. To do so, your organization needs to use the report action with its duplicate rules.

Duplicate Error Logs

If your organization uses Data.com Duplicate Management, you can view any system errors that prevent the duplicate rules or matching rules from running successfully.

How Duplicate Management Affects Your Users

When you've set up and activated Duplicate Manage features in Salesforce, here's what your users see when they try to enter data for or save a record identified as a possible duplicate.

Duplicate Rules

Duplicate rules are used to control whether and when you can save duplicate records within Salesforce.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Duplicate rules tell Salesforce what action to take when you attempt to create a duplicate record. Each duplicate rule requires at least one matching rule to identify which existing records are possible duplicates.

You can configure your duplicate rule to do something when a record is created and edited. However, the rule only runs for edited records if the fields being edited are included in the associated matching rule.

Starting in Spring '15, all new Salesforce orgs come with standard duplicate rules already set up and activated for accounts, contacts, and leads. We recommend that you use the standard duplicate rules, because they're designed to work with the standard matching rules to return the best possible match candidates. You can deactivate the standard duplicate rules at any time. You can also create custom duplicate rules.

Example: The duplicate rule can block you from saving records that have been identified as possible duplicates or allow them to save them anyway. Both the Block and Allow options include an alert, which tells you why you can't save the record and what you need to do. The Allow option includes the ability to report on the duplicate records.

SEE ALSO:

Create or Edit Duplicate Rules

Manage Duplicate Records in Salesforce

Matching Rules

Matching rules are used to identify duplicate records within Salesforce.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Watch a video: Understanding Matching Rules

A matching rule is made up of individual fields that are assembled into an equation. Each field contains matching criteria that tell the rule how to compare the fields and what conditions need to be met for the specific field to be considered a match.

After a matching rule is activated, one or more match keys are automatically created and applied to existing records. (Also known as indexing, this process improves performance and returns a better set of match candidates because the matching rule is only looking for duplicates among records with the same match key.)

When the matching rule is run, it compares the record's match keys against those for existing records. Then, for records that share the same match keys, the matching rule uses matching algorithms to compare fields and determine how closely the fields, and ultimately the records, match. If two records' don't share the same match keys, they are not considered duplicates and the matching algorithms will not even be applied to them.

Example: A simple matching rule might specify that if two records' `Email` and `Phone` values match exactly, they are possible duplicates. Or you can use a variety of "fuzzy" matching methods to compare the fields.

Use matching rules with duplicate rules to manage whether and when users are allowed to create duplicate records within Salesforce.

You can use the standard matching rules or create your own custom matching rule. We recommend you use the standard matching rules because they've been carefully designed to return the best possible set of match candidates.

SEE ALSO:

Create or Edit Custom Matching Rules

Matching Rule Reference

Duplicate Record Sets

Quickly see a list of duplicate records, grouped into duplicate sets, by clicking the Duplicate Record Sets tab. To do so, your organization needs to use the report action with its duplicate rules.

When a user saves a record that's identified as a duplicate by a duplicate rule with the report action:

- The saved record and all its duplicates, up to 100, will be assigned to a new or existing duplicate record set.
- The saved record and each of its duplicates will be listed as a duplicate record item within the duplicate record set.
- If the duplicate rule is configured to find duplicates across objects, all cross-object duplicates will be listed as duplicate record items within the duplicate record set.

Duplicate record sets and duplicate record items can be used to do the following.

- Create custom report types
- Create custom fields
- Write validation rules, triggers, and workflow rules
- Modify the fields that can appear on the respective page layouts

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

SEE ALSO:

Considerations for Using Duplicate Management

Duplicate Error Logs

If your organization uses Data.com Duplicate Management, you can view any system errors that prevent the duplicate rules or matching rules from running successfully.

From Setup, enter *`Duplicate Error Logs`* in the `Quick Find` box, then select **Duplicate Error Logs**. There, you can see which, if any, errors occurred. Error logs are deleted after 90 days.

Example: Here are some scenarios that could produce an error on the log.

- The match engine used for fuzzy matching is temporarily unavailable. Therefore, any matching rules that include fuzzy matching methods will not run.
- The Report action on duplicate rules fails because the system is unable to create a duplicate record set.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

How Duplicate Management Affects Your Users

When you've set up and activated Duplicate Manage features in Salesforce, here's what your users see when they try to enter data for or save a record identified as a possible duplicate.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

IN THIS SECTION:

How Duplicate Management Affects Your Users in Salesforce Classic

When you've created and activated duplicate rules and your users try to save a record that's identified as a possible duplicate, users are given guidance on how to proceed. This is what they see in Salesforce Classic.

How Duplicate Management Affects Your Users in Lightning Experience

In Lightning Experience, when you've created and activated duplicate rules, duplicates are detected even before a record is saved. It's like a magic show without the cape and wand! If your users try to enter data on a record, edit data on a record, or save a record identified as a possible duplicate, here's what they see.

SEE ALSO:

Manage Duplicate Records in Salesforce

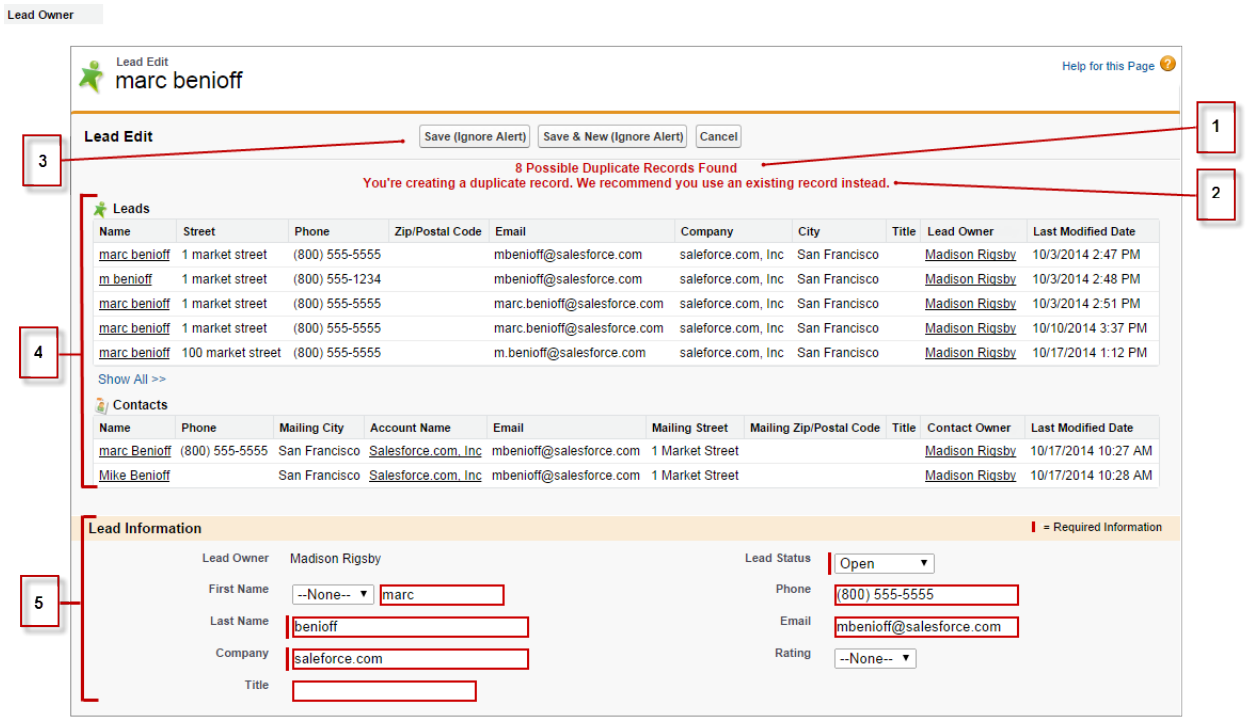
How Duplicate Management Affects Your Users in Salesforce Classic

When you've created and activated duplicate rules and your users try to save a record that's identified as a possible duplicate, users are given guidance on how to proceed. This is what they see in Salesforce Classic.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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



- All duplicate rules include a system-generated message (1) that tells the user how many possible duplicates were found. The number of possible duplicates includes only the records the user has access to, even if the duplicate rule's record-level security was set to *Bypass sharing rules*. (The *Bypass sharing rule* option tells the associated matching rule to compare all records, regardless of the user's access.) If the user doesn't have access to any of the records that are identified as possible duplicates, then this message just says there are duplicates detected and the number of duplicates isn't included. The list of possible duplicates displayed only includes records the user has access to.
- If your duplicate rule includes an alert, it will appear beneath the system-generated message (2).
- If your duplicate rule allows users to save a record even though it might be a possible duplicate, the **Save (Ignore Alert)** button is present (3). If your duplicate rule blocks users from saving a record that is a possible duplicate, the **Save** button is present but the record cannot be saved successfully until the user makes the necessary changes to the record so it's no longer flagged as a possible duplicate.
- The list of possible duplicates (4) includes only records the user has access to. The fields shown in the list include only fields the user has access to (up to the first 7 fields that were compared by the associated matching rule). A maximum of 5 records are displayed in this list, but if more than 5 duplicates are found, users can click **Show All >>** to see full list of records, up to 100. Records are listed in the order they were last modified. Users can go directly to one of the records in the list by clicking on its link.
- The highlighted fields (5) are the fields that were compared by the associated matching rule and determined to match.

How Duplicate Management Affects Your Users in Lightning Experience

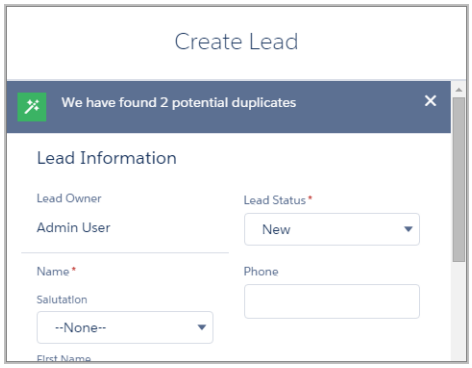
In Lightning Experience, when you've created and activated duplicate rules, duplicates are detected even before a record is saved. It's like a magic show without the cape and wand! If your users try to enter data on a record, edit data on a record, or save a record identified as a possible duplicate, here's what they see.

As soon as a user enters or edits data on a record, duplicate rules run. A general alert appears if duplicates are detected—not the customizable alert associated with your duplicate rules. The alert includes the number of potential duplicates. This number includes only the records the user has access to, even if the duplicate rule's record-level security was set to `Bypass sharing rules`. Users can click the alert to review the matching Salesforce records.

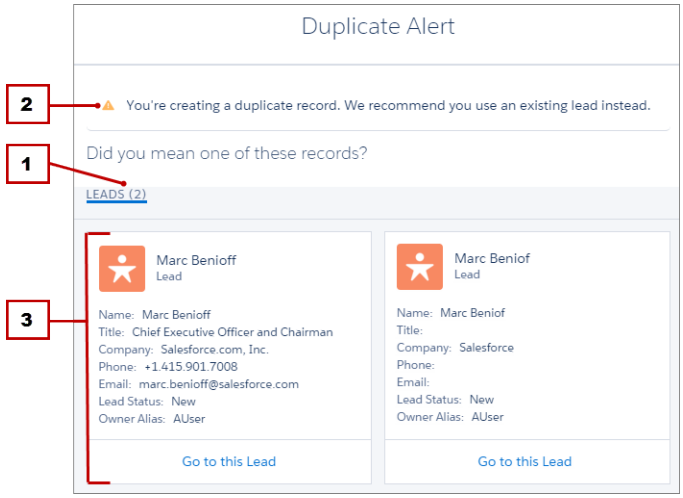
EDITIONS

Available in: Salesforce Classic and Lightning Experience

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



If your users try to save a record identified as a possible duplicate, here's what they see.



- All duplicate rules include a system-generated message (1) that tells the user how many possible duplicates were found. The number of possible duplicates includes only the records the user has access to, even if the duplicate rule's record-level security was set to `Bypass sharing rules`. (The `Bypass sharing rule` option tells the associated matching rule to compare all records, regardless of the user's access.) If the user doesn't have access to any of the records that are identified as possible duplicates, then this message just says there are duplicates detected and the number of duplicates isn't included. The list of possible duplicates displayed only includes records the user has access to.
- If your duplicate rule includes an alert, it will appear above the system-generated message (2).

- If your duplicate rule allows users to save a record even though it might be a possible duplicate, they can close this dialog and save the record like they normally would. If your duplicate rule blocks users from saving a record that is a possible duplicate, the record cannot be saved successfully until the user makes the necessary changes to the record so it's no longer flagged as a possible duplicate.
- The list of possible duplicates (3) includes only records the user has access to. The fields shown in the list include only fields the user has access to (up to the first 7 fields that were compared by the associated matching rule). Records are listed in the order they were last modified. Users can go directly to one of the records in the list by clicking on its link.

Set Up Duplicate Management in Salesforce

To use Data.com Duplicate Management in your organization, you need two separate rules: a duplicate rule and a matching rule. The duplicate rule tells Salesforce what action to take when duplicates are identified. The matching rule defines how records are compared to one another to identify possible duplicates.

Important: Starting in Spring '15, all new Salesforce orgs come with Duplicate Management features set up and activated for accounts, contacts, and leads. New orgs come with standard account, contact, and lead duplicate and matching rules.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

IN THIS SECTION:

Create or Edit Duplicate Rules

Use duplicate rules to define what happens when a user tries to save a duplicate record.

Create or Edit Custom Matching Rules

Use matching rules to determine how two records are compared and identified as duplicates.

Create Custom Report Types for Duplicate Record Reports

If your organization uses the Report action with its duplicate rules, you can run reports to analyze the quality of your data and to see how well your duplicate rules are working. That way, you can fine tune your duplicate rules if needed. First, you'll need to set up the appropriate custom report types.

Create or Edit Duplicate Rules

Use duplicate rules to define what happens when a user tries to save a duplicate record.

Watch a demo: Managing Duplicate Records in Salesforce with Duplicate Rules

In order for users to see the list of possible duplicates detected by the duplicate rule, they must have read access to the object defined in the rule.

1. From Setup, enter *Duplicate Rules* in the Quick Find box, then select **Duplicate Rules**.
2. To edit an existing rule, click the rule name, then click **Edit**. To create a new rule, click **New Rule** , then select the object you want the rule to apply to.
3. Enter the rule details, including the rule's name, description, and record-level security settings.
4. Select which action will occur when a user tries to save a duplicate record.

   If the action includes an alert to users, we'll provide default alert text that you can customize. Only the Allow action includes the report option.
5. In the Matching Rules section, first select the object that records will be compared with. Then select which matching rule will determine how records are identified as duplicates.

   The list includes all available matching rules for the selected object. If none of the matching rules in the list are what you want, select Create New Matching Rule.

   Tip: We recommend you use the standard matching rules because they've been carefully designed to return the best possible set of match candidates. Just be sure you've activated them.

   If, however, you decide to create a new matching rule, we recommend you first finish creating your duplicate rule. Then create and activate the new matching rule. When you come back to the duplicate rule, it will automatically have the newly created matching rule associated it, as long as it didn't already have an associated matching rule.
6. Make sure you've selected the field mapping for each matching rule, if needed.

   If the matching rule is comparing records from two different objects or uses custom fields:

   - You'll need to decide how you want the fields from the first object to be compared to the fields from the second object. For example, you might map a custom field called Work Email to the standard Email field.
   - Some data may be truncated prior to matching two text fields with different maximum lengths.
7. If you want your duplicate rule to run only if specific conditions are met, specify the conditions.

   For example, you could add a condition that tells the rule to run only if the record was entered by a user with a certain profile or role, or if the record includes a specific country or state.
8. Save the rule.
9. Activate the rule.

   For the activation to succeed, all associated matching rules must be active.
10. If you have more than one active duplicate rule for a particular object, you may want to adjust the order in which the rules are processed. You can reorder rules by clicking **Reorder** from any rule's detail page.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create, edit, or delete duplicate rules:
- "Customize Application"

To activate and deactivate duplicate rules:
- "Customize Application"

To view duplicate rules:
- "View Setup and Configuration"

Tip: If the first duplicate rule finds a match for a particular record, that record will not be evaluated by subsequent duplicate rules. Therefore, you should order your duplicate rule so that rules with the Block action are run before rules with the Allow action.

SEE ALSO:

Duplicate Rules

Matching Rules

Create or Edit Custom Matching Rules

Use matching rules to determine how two records are compared and identified as duplicates.

Watch a Demo (3:39)

1. From Setup, enter *Matching Rules* in the Quick Find box, then select **Matching Rules**.
2. If editing an existing matching rule, make sure the rule is inactive.
3. Click **New Rule** or **Edit** next to the existing rule you want to edit.
4. Select which object this matching rule will apply to.
5. Enter a name and description for the rule.
6. Enter the matching criteria.

   The matching criteria is where you define which fields to compare and how. To add additional fields (up to 10 total) click **Add Filter Logic...** and then **Add Row**.
7. If you need to adjust the matching equation, click **Add Filter Logic...**. Here you can, for example, manually change an AND expression to an OR expression.
8. Save the rule.
9. Activate the rule.

   The activation process may take some time, so we'll send you an email when the process is complete and your matching rule is ready to use.

After the matching rule is active, it's available to use with other Data.com Duplicate Management tools. For example, using a matching rule with a duplicate rule tells Salesforce to take certain actions when users try to save a record the matching rule has identified as a duplicate.

SEE ALSO:

Matching Rules

Matching Rule Reference

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create, edit, or delete matching rules:

- "Customize Application"

To activate and deactivate matching rules:

- "Customize Application"

To view matching rules:

- "View Setup and Configuration"

Create Custom Report Types for Duplicate Record Reports

If your organization uses the Report action with its duplicate rules, you can run reports to analyze the quality of your data and to see how well your duplicate rules are working. That way, you can fine tune your duplicate rules if needed. First, you'll need to set up the appropriate custom report types.

The only records that will appear in these reports are:

- Records identified as duplicates by duplicates rules that include the report action.
- Records that were manually added to the Duplicate Record Set object.

1. Make sure you're familiar with custom report types and the general steps for creating and maintaining them.
2. Create custom report types with the appropriate object relationships and configure them as necessary.

   Here are some examples of custom report types to get you started.

Report Type	Possible Use	A (Primary Object)	B	Additional Steps
Account Duplicates	Create reports on the duplicate accounts that were found by your duplicate rules.	Accounts	Duplicate Record Items	
Contact Duplicates	Create reports on the duplicate contacts that were found by your duplicate rules.	Contacts	Duplicate Record Items	
Lead Duplicates	Create reports on the duplicate leads that were found by your duplicate rules.	Leads	Duplicate Record Items	
All Duplicates	Create reports to see how well your duplicate rules are performing.	Duplicate Record Set	Duplicate Record Items	Add the `Duplicate Rule Name` lookup field to the Duplicate Record Set page layout.

3. Deploy the report types you want to make available to users.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To create or update custom report types:
- "Manage Custom Report Types"

To delete custom report types:
- "Modify All Data"

4. Let users know that they can create reports using these custom report types.

SEE ALSO:

Duplicate Record Sets

Matching Rule Reference

Here's some additional information that will help you understand how matching rules work and how to use them.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

IN THIS SECTION:

Standard Matching Rules

We've provided several standard matching rules that you can use with Data.com Duplicate Management tools, such as duplicate rules. Each standard matching rule has been carefully designed to return the best possible set of match candidates for accounts, contacts, or leads.

Matching Criteria for Matching Rules

Matching rules use criteria to determine how closely a field on a new or edited record matches the same field on an existing record, and, ultimately, whether the two records are duplicates. When you create a custom matching rule, you need to define certain criteria. For standard matching rules, the criteria are already defined for you.

Matching Methods Used with Matching Rules

The matching method is the part of the matching rule's matching criteria that determines how a specific field in one record is compared to the same field in another record. Each matching method is further defined by normalization criteria, match key definitions, matching algorithms, and other criteria.

Matching Algorithms Used with Matching Methods

The matching method and its corresponding matching algorithms are part of the matching rule's matching criteria. They help determine how a specific field in one record is compared to the same field in another record and whether the fields are considered matches.

Match Keys Used with Matching Rules

Match keys increase the effectiveness of matching rules. Review how match keys are used to create match key values for standard matching rules. By understanding match keys, you'll get a better sense of how duplicate detection works.

Normalization Criteria for Matching Rule Match Keys

As part of the process of creating match key values, matching rule field values are normalized. How a field value is normalized depends on several factors, including the matching method for that field, as specified in the matching rule. In addition, some commonly-used fields, which are used in the standard matching rules, are specially normalized to optimize duplicate detection.

Matching Examples

Check out some examples of matching rules in action to help you understand how records are compared and evaluated as duplicates.

Standard Matching Rules

We've provided several standard matching rules that you can use with Data.com Duplicate Management tools, such as duplicate rules. Each standard matching rule has been carefully designed to return the best possible set of match candidates for accounts, contacts, or leads.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

IN THIS SECTION:

Standard Account Matching Rule

Like all matching rules, the standard matching rule used for account records is made up of fields that are arranged into an equation. Each field contains matching criteria that the rule uses to determine how closely the field matches the same field in an existing record, and ultimately whether the record is a match.

Matching Equation

Important: In order for the Standard Account Matching Rule to return matches accurately, the new or edited record must include a value in the `Account Name` and either the `City` or `ZIP` fields.

Rule Name	Matching Equation
Standard Account Matching Rule	(*`Account Name`* AND *`Billing Street`*) OR (*`Account Name`* AND *`City`*) OR (*`Account Name`* AND *`ZIP`*) OR (*`Account Name`* AND *`Phone`*) OR (*`Website`* AND *`Phone`*) OR (*`Website`* AND *`Billing Street`*)

Matching Criteria

For a definition of each matching criterion, see Matching Criteria for Matching Rules on page 455.

Field	Matching Algorithms	Scoring Method	Threshold	Blank Fields	Special Handling
`Account Name`	Acronym Edit Distance	Maximum	70	Don't match	Removes words such as `Inc` and `Corp` before comparing fields. Also, company names are normalized. For example, `1st`

Field	Matching Algorithms	Scoring Method	Threshold	Blank Fields	Special Handling
	Exact				`National Bank` is normalized to `First National Bank`.
`Phone`	Exact	Weighted Average	80	Don't match on all sections expect Area Code, which ignores blank fields	Phone numbers are broken into sections and compared by those sections. Each section has its own matching method and match score. The section scores are weighted to come up with one score for the field. This process works best with North American data. • International code (Exact, 10% of field's match score) • Area code (Exact, 50% of field's match score) • Next 3 digits (Exact, 30% of field's match score • Last 4 digits (Exact, 10% of field's match score) For example, suppose these two phone numbers are being compared: *`1-415-555-1234`* and *`1-415-555-5678`*. All sections match exactly *except* the last 4 digits, so the field has a match score of 90, which is considered a match because it exceeds the threshold of 80.
`Billing Street`	Edit Distance Exact	Weighted Average	80	Don't match	Addresses are broken into sections and compared by those sections. Each section has its own matching method and match score. The section scores are weighted to come up with one score for the field. This process works best with North American data. • Street Number (Exact, 20% of field's match score) • Street Name (Edit Distance, 50% of field's match score) • Street Suffix (Exact, 15% of field's match score) • Suite Number (Exact, 15% of field's match score) For example, suppose these two billing streets are being compared: *`123 Market Street, Suite 100`* and *`123 Market Drive, Suite 300`*. Because only the street number and street name match, the field has a match score of 70, which is not considered a match because it's less than the threshold of 80.
`ZIP`	Exact	Weighted Average	80	Don't match	ZIP codes are broken into sections and compared by those sections. Each section has its own matching method and match score. The section scores are weighted to come up with one score for the field. • First 5 digits (Exact, 90% of field's match score) • Next 4 digits(Exact, 10% of field's match score) For example, suppose these two ZIP codes are being compared: *`94104-1001`* and *`94104`*.

Field	Matching Algorithms	Scoring Method	Threshold	Blank Fields	Special Handling
					Because only the first 5 digits match, the field has a match score of 90, which is considered a match because it exceeds the threshold of 80.
`City`	Edit Distance Exact	Maximum	85	Don't match	
`Website`	Exact	Maximum	100	Don't match	Only the website domain is compared. For example, a field value `http://www.salesforce.com` becomes `salesforce.com`.

SEE ALSO:

Matching Rule Reference

Standard Contact and Lead Matching Rule

Like all matching rules, the standard matching rule used for contact and lead records is made up of fields that are arranged into an equation. Each field also contains matching criteria that the rule uses to determine how closely the field matches the same field in an existing record, and ultimately whether the record is a match.

Matching Equation

Rule Name	Matching Equation
Standard Contact Matching Rule Standard Lead Matching Rule	(*First Name* AND *Last Name* AND *Title* AND *Company Name*) OR (*First Name* AND *Last Name* AND *Email*) OR (*First Name* AND *Last Name* AND *Phone* AND *Company Name*) OR (*First Name* AND *Last Name* AND *Mailing Street* AND (*City* OR *ZIP* OR *Phone*) OR (*First Name* AND *Last Name* AND *Mailing Street* AND *Title*) OR (*First Name* AND *Last Name* AND *Title* AND *Email*) OR (*First Name* AND *Last Name* AND *Phone*)

Matching Criteria

For a definition of each matching criteria, see Matching Criteria for Matching Rules on page 455.

Fields on Contacts	Fields on Leads	Matching Algorithms	Scoring Method	Threshold	Blank Fields	Special Handling
First Name	First Name	Exact Initials Jaro-Winkler Distance Metaphone 3 Name Variant	Maximum	85	Don't match (Ignores blank fields when Email is included in field grouping)	If record contains a value for the both `First Name` and `Last Name` fields, those values will be transposed to account for possible data entry mistakes. For example, if the first name is *`George`* and the last name is *`Michael`*, the matching rule will also evaluate first name as *`Michael`* and the last name as *`George`*.
Last Name	Last Name	Exact Keyboard Distance Metaphone 3	Maximum	90	Don't match (Ignores blank fields when Email is included in field grouping)	If record contains a value for the both `First Name` and `Last Name` fields, those values will be transposed to account for possible data entry mistakes. For example, if the first name is *`George`* and the last name is *`Michael`*, the matching rule will also evaluate first name as *`Michael`* and the last name as *`George`*.
Title	Title	Acronym Exact Kullback-Liebler Distance	Maximum	50	Don't match	
Account Name	Company	Acronym Edit Distance Exact	Maximum	70	Don't match	
Email	Email	Exact	Maximum	100	Don't match	
Phone	Phone	Exact	Weighted Average	80	Don't match on all sections expect Area Code, which ignores blank fields	Phone numbers are broken into sections and compared by those sections. Each section has its own matching method and match score. The section scores are weighted to come up with one score for the field. This process works best with North American data. • International code (Exact, 10% of field's match score) • Area code (Exact, 50% of field's match score) • Next 3 digits (Exact, 30% of field's match score • Last 4 digits (Exact, 10% of field's match score) For example, suppose these two phone numbers are being compared: *`1-415-555-1234`* and *`1-415-555-5678`*.

Fields on Contacts	Fields on Leads	Matching Algorithms	Scoring Method	Threshold	Blank Fields	Special Handling
						All sections match exactly *except* the last 4 digits, so the field has a match score of 90, which is considered a match because it exceeds the threshold of 80.
Mailing Street	Street	Exact	Weighted Average`	80	Don't match	Addresses are broken into sections and compared by those sections. Each section has its own matching method and match score. The section scores are weighted to come up with one score for the field. This process works best with North American data. • Street Name (Edit Distance, 50% of field's match score) • Street Number (Exact, 20% of field's match score) • Street Suffix (Exact, 15% of field's match score) • Suite Number (Exact, 15% of field's match score) For example, suppose these two addresses are being compared: `123 Market Street, Suite 100` and `123 Market Drive, Suite 300`. Because only the street number and street name match, the field has a match score of 70, which is not considered a match because it's less than the threshold of 80.
Mailing ZIP/Postal Code	ZIP/Postal Code	Exact	Weighted Average	80		ZIP codes are broken into sections and compared by those sections. Each section has its own matching method and match score. The section scores are weighted to come up with one score for the field. • First 5 digits (Exact, 90% of field's match score) • Next 4 digits(Exact, 10% of field's match score)
Mailing City	City	Edit Distance Exact	Maximum	85	Don't match	

SEE ALSO:

Matching Rule Reference

Matching Criteria for Matching Rules

Matching rules use criteria to determine how closely a field on a new or edited record matches the same field on an existing record, and, ultimately, whether the two records are duplicates. When you create a custom matching rule, you need to define certain criteria. For standard matching rules, the criteria are already defined for you.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Criterion	Definition	Automatically Defined for Custom Matching Rules
Field	Indicates which field to compare. When selecting fields, keep in mind that: • The available fields depend on which object the matching rule applies to and include both standard and custom fields. • The supported input field types are email, lookup relationship, master-detail relationship, number, phone, standard picklists, custom picklists (single-select only), text, and URL. • An auto-numbered lookup relationship field cannot be used in a matching rule. • If you enable `State` and `Country` picklists for your organization, we recommend using **State/Province Code** and **Country Code** in your matching rules. These fields yield better duplicate detection results than the state and country text fields.	
Matching Method	Defines the method for how the fields are compared. We've provided an exact matching method that can be used for almost any field, including custom fields. A fuzzy matching method is available for commonly used standard fields. Each matching method is further defined by normalization and match key definitions, matching algorithms, and other criteria. For more information about matching methods, see Matching Methods Used with Matching Rules on page 457.	
Match Blank Fields	Specifies how blank fields affect whether the 2 fields being compared are considered matches. If you select the `Match Blank Fields` checkbox for any field, and that field is blank in *both* records being compared, the fields are considered matches. If, however, you select the `Match Blank Fields` checkbox for any field, and that field is blank in *only one* of the records being compared, the fields are not considered matches. If you don't select the `Match Blank Fields` checkbox for any field, and that field is blank in *both* records being compared, the fields are *not* considered matches.	

Criterion	Definition	Automatically Defined for Custom Matching Rules
Match Key	A formula that allows the matching rule to quickly return a list of possible duplicates. Once a matching rule is activated, match keys are used to generate match key values for all records. When a matching rule runs, it compares the match key values of the saved record with existing records. If the saved record has the same match key value as an existing record, it's a potential duplicate and evaluated further. If the saved record has a unique match key value, it's not considered a duplicate. This process improves the speed and performance of duplicate detection. For more information about match keys, including examples, see Match Keys Used with Matching Rules on page 461.	✅
Matching Algorithm	Defines the logic that determines whether 2 fields match. For the Exact matching method, the Exact matching algorithm is automatically used. For the Fuzzy matching method, various fuzzy matching algorithms can be used. Each matching algorithm used is automatically given a match score based on how closely it's able to match the two fields. For example, if you select Exact matching and the two fields match, the match score is 100. If the 2 fields don't match, the match score is 0. For more information about matching algorithms, see Matching Algorithms Used with Matching Methods on page 459.	✅
Scoring Method	Determines how the matching algorithms' match scores are calculated to come up with one match score for the field. Each matching algorithm used is automatically given a match score based on how closely it's able to match the two fields. Scoring method is used only by the standard matching rules. `Average`: Uses the average match score. `Maximum`: Uses the highest match score. `Minimum:` Uses the lowest match score. `Weighted Average` Uses the weight of each matching method to determine the average match score.	✅
Threshold	Determines the minimum match score needed for the field to be considered a match. The field is automatically given a match score based on how closely it matches the same field in an existing record.	✅

SEE ALSO:

Matching Rule Reference
Considerations for Using Duplicate Management

Matching Methods Used with Matching Rules

The matching method is the part of the matching rule's matching criteria that determines how a specific field in one record is compared to the same field in another record. Each matching method is further defined by normalization criteria, match key definitions, matching algorithms, and other criteria.

The *Exact* matching method looks for strings that match a pattern exactly. If you're using international data, we recommend you use the Exact matching method with your matching rules. We've provided an exact matching method that can be used for almost any field, including custom fields.

The *Fuzzy* matching methods look for strings that match a pattern approximately. A fuzzy matching method is available for commonly used standard fields on accounts, contacts, and leads.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Matching Method	Matching Algorithms	Scoring Method	Threshold	Special Handling
Exact	Exact			
Fuzzy: First Name	Exact Initials Jaro-Winkler Name Variant	Maximum	85	The `Middle Name` field, if used in your matching rule, is compared by the Fuzzy: First Name matching method.
Fuzzy: Last Name	Exact Keyboard Distance Metaphone 3	Maximum	90	
Fuzzy: Company Name	Acronym Exact Syllable Alignment	Maximum	70	Removes words such as `Inc` and `Corp` before comparing fields. Also, company names are normalized. For example, `IBM` is normalized to `International Business Machines`.
Fuzzy: Phone	Exact	Weighted Average	80	Phone numbers are broken into sections and compared by those sections. Each section has its own matching method and match score. The section scores are weighted to come up with one score for the field. This process works best with North American data. • International code (Exact, 10% of field's match score) • Area code (Exact, 50% of field's match score)

Matching Method	Matching Algorithms	Scoring Method	Threshold	Special Handling
				• Next 3 digits (Exact, 30% of field's match score • Last 4 digits (Exact, 10% of field's match score) For example, suppose these two phone numbers are being compared: `1-415-555-1234` and `1-415-555-5678`. All sections match exactly *except* the last 4 digits, so the field has a match score of 90, which is considered a match because it exceeds the threshold of 80.
Fuzzy: City	Edit Distance Exact	Maximum	85	
Fuzzy: Street	Exact	Weighted Average	80	Addresses are broken into sections and compared by those sections. Each section has its own matching method and match score. The section scores are weighted to come up with one score for the field. This process works best with North American data. • Street Name (Edit Distance, 50% of field's match score) • Street Number (Exact, 20% of field's match score) • Street Suffix (Exact, 15% of field's match score) • Suite Number (Exact, 15% of field's match score) For example, suppose these two billing streets are being compared: `123 Market Street, Suite 100` and `123 Market Drive, Suite 300`. Because only the street number and street name match, the field has a match score of 70, which is not considered a match because it's less than the threshold of 80.
Fuzzy: ZIP	Exact	Weighted Average	80	ZIP codes are broken into sections and compared by those sections. Each section has its own matching method and match score. The section scores are weighted to come up with one score for the field.

Matching Method	Matching Algorithms	Scoring Method	Threshold	Special Handling
				• First 5 digits (Exact, 90% of field's match score) • Next 4 digits(Exact, 10% of field's match score) For example, suppose these two ZIP codes are being compared: `94104-1001` and `94104`. Because only the first 5 digits match, the field has a match score of 90, which is considered a match because it exceeds the threshold of 80.
Fuzzy: Title	Acronym Exact Kullback-Liebler Distance	Maximum	50	

SEE ALSO:

Matching Criteria for Matching Rules

Matching Algorithms Used with Matching Methods

Matching Algorithms Used with Matching Methods

The matching method and its corresponding matching algorithms are part of the matching rule's matching criteria. They help determine how a specific field in one record is compared to the same field in another record and whether the fields are considered matches.

We've provided an exact matching method and a variety of fuzzy matching methods. If the exact matching method is selected, then the exact matching algorithm is automatically used to compare the fields. If one of the fuzzy matching method is selected, then a variety of fuzzy matching algorithms is used to compare the fields. A field can be compared using more than one matching algorithm, and a matching score is given to each matching algorithm based on how closely it's able to match the fields. The fields being compared by the matching algorithms are *not* case sensitive.

For more information about the matching methods, see Matching Methods Used with Matching Rules on page 457.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Matching Algorithms Available with Exact Matching Method

Matching Algorithm	Description
Exact	Determines whether two strings are the same. For example, salesforce.com and Salesforce are not considered a match because they're not exactly the same, and return a match score of 0.

Matching Algorithms Available with Fuzzy Matching Methods

Matching Algorithm	Description
Acronym	Determines whether a business name matches its acronym. For example, Advanced Micro Devices and its acronym AMD are considered a match and return a match score of 100.
Edit Distance	Determines the similarity between two strings based on the number of deletions, insertions, and character replacements needed to transform one string into the other. For example, VP Sales matches VP of Sales with match score of 73.
Initials	Determines the similarity of two sets of initials in personal names. For example, the first name Jonathan and its initial J match and return a match score of 100.
Jaro-Winkler Distance	Determines the similarity between two strings based on the number of character replacements needed to transform one string into the other. This method is best for short strings, such as personal names. For example, Johnny matches Johny with a match score of 97.
Keyboard Distance	Determines the similarity between two strings based on the number of deletions, insertions, and character replacements needed to transform one string into the other, weighted by the position of the keys on the keyboard.
Kullback Liebler Distance	Determines the similarity between two strings based on the percentage of words in common. For example Director of Engineering matches Engineering Director with a match score of 65.
Metaphone 3	Determines the similarity between two strings based on their sounds. This algorithm attempts to account for the irregularities among languages and works well for first and last names. For example, Joseph matches Josef with a match score of 100.
Name Variant	Determines whether two names are variation of each other. For example, Bob is a variation of Robert and returns a match score of 100. Bob is not a variation of Bill and returns a match score of 0.
Syllable Alignment	Determines the similarity between two strings based on their sounds. First, the character strings are converted into syllables strings. Then the syllable strings are also compared and scored using the Edit Distance algorithm. This matching algorithm works well for company names. For example, Syllable Alignment gives Department of Energy and Department of Labor have a relatively low match score of 59 because the syllable sequences of these two company names differ more than their character sequences (“energy” sounds very different than “labor”). Edit Distance gives the two strings a score of 74. Therefore, Syllable Alignment works better because the two strings should not be considered a match.

SEE ALSO:

- Matching Rule Reference
- Matching Methods Used with Matching Rules

Match Keys Used with Matching Rules

Match keys increase the effectiveness of matching rules. Review how match keys are used to create match key values for standard matching rules. By understanding match keys, you'll get a better sense of how duplicate detection works.

A *match key* is a formula that allows a matching rule to quickly return a list of possible duplicates.

Once a matching rule is activated, match keys are used to create match key values for all records. When a matching rule runs, it compares the match key values of the saved record and existing records. If the saved record has the same match key value as an existing record, it's a potential duplicate and evaluated further. If the saved record has a unique match key value, it's not considered a duplicate. On rare occasions, the use of match keys causes duplicates to be missed. It almost never happens, and we're pretty sad when it does. Fortunately, the performance benefits of using match keys greatly outweighs the drawbacks.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

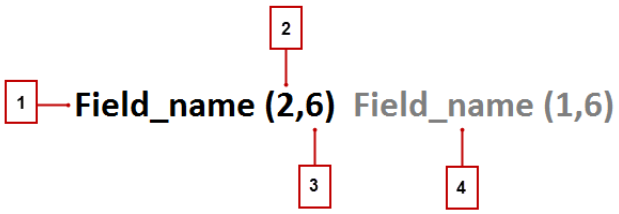
How Match Keys and Match Key Values Are Created

1. The matching rule equation (that is, the arrangement of fields) is rewritten into a standardized format that translates OR statements into AND statements.
2. Values for fields in the matching rule are normalized.
3. A match key is created using the field combinations specified in the standardized field format. Matching rules can have multiple match keys. For standard matching rules or custom rules with standard field combinations, pre-defined match keys are used.
4. The match key is used to combine normalized field values for each record. And, voila, glorious match key values are born!

Note: We currently don't create match keys for the `Title` and `Address` fields. Therefore, if those fields are included in your matching rule, they won't generate match keys.

Match Key Notation

The common match key notation shows which fields and which characters in those fields are used in the match key.



- The field used in the match key (1)
- Number of words (or tokens) in the field value to include in match key (2). If no number is present, then all words are included.
- Number of characters per word to include in the match key (3). If no number is present, then all characters are included.
- Additional field used in the match key (4)

Note: Each custom matching rule can have a maximum of 10 match keys; you're prevented from saving a matching rule that would require more.

Pre-Defined Match Keys for Standard Matching Rules

Standard matching rules use pre-defined match keys.

Match Key Notation	Objects Applied To	Match Key Value Examples
Company (2,6) City (_, 6)	Account	Account: Orange Sporting Company = orangesporti City: San Francisco = sanfra Key: orangesportisanfra
Company (2,6) ZIP (1,3)	Account	Account Name: salesforce.com = orangesports ZIP: 94105-5188 = 941 Key: salesf941
Email	Contact Lead	Email: john_doe@us.ibm.com = johndoe@ibm.com Key: johndoe@ibm.com
First_Name (1,1) Last_Name Email	Contact Lead	First Name: John = j Last: Doe = doe = t (with double metaphone applied) Email: john_doe@us.salesforce.com = johndoe@salesforce.com Key: jt@salesforce.com
First_Name (1,1) Last_Name Company (2,5)	Contact Lead	First Name: Marc = m Last Name: Benioff = pnf (with double metaphone applied) Company: salesforce.com = sales Key: mpnfsales
First_Name (1,1) Last_Name Phone	Contact Lead	First Name: Marc = m Last Name: Benioff = pnf (with double metaphone applied) Phone: 1-415-555-1234 = 415555 Key: mpnf415555
Website City (_,6)	Account	Website: https://www.salesforce.com = salesforce.com City: San Francisco = sanfra Key: salesforce.comsanfra
Website ZIP (1,3)	Account	Website: https://www.salesforce.com = salesforce.com ZIP: 94105-5188 = 941 Key: salesforce.com941

Custom matching rules may also use these pre-defined match keys. For example, assume the matching rule equation for a custom contact matching rule is (`First Name` AND `Last Name` AND `Company`), and the Fuzzy matching method is selected for at least one of the fields. Then, the notation for its match key will be: First_Name (1,1) Last_Name Company (2,6).

SEE ALSO:

- Matching Rule Reference
- Matching Criteria for Matching Rules
- Normalization Criteria for Matching Rule Match Keys

Normalization Criteria for Matching Rule Match Keys

As part of the process of creating match key values, matching rule field values are normalized. How a field value is normalized depends on several factors, including the matching method for that field, as specified in the matching rule. In addition, some commonly-used fields, which are used in the standard matching rules, are specially normalized to optimize duplicate detection.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Field	Normalization Details	Applies to Standard *and* Custom Matching Rules?	Examples
`Company`	Expands acronyms. Lowercases all characters. Removes suffixes, such as `Corporation`, `Incorporated`, `Inc`, `Limited`, `Ltd`. Removes stopwords `and`, `the`, `of`. Removes special characters and accents.	Yes. But on custom matching rules, *`Fuzzy: Company`* must be selected for the Matching Method.	IBM = international business machines Intel Corp. = intel
`First Name`	Replaces first name with alias, if applicable. Removes salutations, special characters, and accents. Keeps only the first letter of the first word and lowerycases this letter.	Yes. But on custom matching rules, *`Fuzzy: First Name`* must be selected for the Matching Method.	Dr. Jane = j Mr. Bob= robert = r
`Last Name`	Removes special characters and suffixes. Replaces consecutive identical consonants with single consonant. Lowercases first letter. After normalization, the double metaphone algorithm is applied so that misspellings and spelling variants are accounted for.	Yes. But on custom matching rules, *`Fuzzy: Last Name`* must be selected for the Matching Method.	O'Reilly, Jr. = oreily (without double metaphone) O'Reilly, Jr. = oreily = arl (with double metaphone)
`Email`	Removes special characters, such as underscores and periods, from both parts of the email address. Retains the "@" character.	No. Only applies to standard matching rules.	john.doe@us.salesforce.com = johndoe@salesforcecom

Field	Normalization Details	Applies to Standard *and* Custom Matching Rules?	Examples
`Phone`	Removes all non-digit and non-alpha characters. For all U.S. phone numbers, converts alpha characters to numeric characters and removes leading international code. Removes last 4 digits.	Yes. But on custom matching rules, *`Fuzzy: Phone`* must be selected for the Matching Method.	1-800-555-1234 = 800555 44 20 0540 0202 = 44200540
`Website`	Removes protocol (http), subdomain (www), and any file path. Then takes only the last two or three tokens, depending on if there are international designations. Retains the periods.	No. Only applies to standard matching rules.	http://www.us.salesforce.com/product = salesforce.com http://www.ox.ac.uk/ = ox.ac.uk

Note: Other fields, including custom fields and fields using the Exact matching method in the matching rule, are normalized by lowercasing all letters and removing leading and trailing spaces.

SEE ALSO:

- Matching Rule Reference
- Matching Criteria for Matching Rules
- Match Keys Used with Matching Rules

Matching Examples

Check out some examples of matching rules in action to help you understand how records are compared and evaluated as duplicates.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Example: **Custom Lead Matching Rule with Fuzzy Matching Methods**

Table 3: Matching Criteria

	Field	Matching Method
1	`Company`	*`Fuzzy: Company Name`*
2	`Email`	*`Exact`*
3	`Phone`	*`Fuzzy: Phone`*
	Matching equation is (`Company` OR `Email`) AND (`Phone`)	

Based on this matching criteria, here's how matching works.

1. **Match key values are generated for existing leads.** Based on the matching equation and the specified matching methods, 2 match keys are created. From these, match key values are generated.

Table 4: Match Keys

Matching Equation in Standardized Format	Match Key	Sample Matching Field Values	Sample Match Key Values
(`Company` AND `Phone`) OR	Company (2,6) Phone	`Company` = Global Guitars Inc. `Phone` = 415-123-4567	globalguitar415123
(`Email` AND `Phone`)	Email Phone	`Email` = sally.smith@globalguitars.com `Phone` = 415-123-4567	sally.smith@globalguitars.com4151234567

2. **Match key values for the new record are generated.** This happens as soon as the new record is saved.

Table 5: New Record

Matching Field Values	Match Key Values
`Company` = Eltie Sports `Email` = john.doe@elitesport.com `Phone` = 1-415-555-1234	eltiesports415555 john.doe@elitesport.com415555

3. **Match key values for the new record are compared with those from existing records.**

Table 6: Existing Records Compared with New Record

Record	Matching Field Values	Match Key Values	Match?
1	`Company` = Elite Sports `Email` = john.doe@elitesports.com `Phone` = 1-415-555-1234	elitesports415555 john.doe@elitesports.com415555	No. Not considered a duplicate.
2	`Company` = Elite Sport `Email` = john.doe@elitesport.com `Phone` = 1-415-555-1234	elitesport415555 john.doe@elitesport.com415555	Yes. The first match key values don't match. However, the second match key values are identical, so the record is considered a potential duplicate. Only one match key value match is needed.

4. **Determine if the new record is a potential duplicate.** Does the new record have the same match key value as an existing record?
   - Yes—The new record is considered a potential duplicate. It's evaluated further using other matching resources, including matching algorithms.
   - No—The new record is not considered a duplicate.

Example: **Custom Contact Matching Rule with Exact Matching Methods**

Table 7: Matching Criteria

	Field	Matching Method
1	`City`	*Exact*
2	`Email`	*Exact*
3	`Phone`	*Exact*
	Matching equation is (`City` OR `Email`) AND (`Phone`)	

Based on this matching criteria, here's how matching works.

1. **Match key values are generated for existing contacts.** Based on the matching equation and the specified matching methods, 2 match keys is created. From these, match key values are generated.

Table 8: Match Key

Matching Equation in Standardized Format	Match Key	Sample Matching Field Values	Sample Match Key Values
(`City` AND `Email`) OR	City Email	`City` = San Francisco `Email` = john.doe@elitesports.com	san francisco john.doe@elitesports.com
(`City` AND `Phone`)	City Phone	`City` = San Francisco `Phone` = 415-555-1234	san francisco 415-555-1234

2. **Match key values for the new record are generated.** This happens as soon as the new record is saved.

Table 9: New Record

Matching Field Values	Match Key Values
`City` = San Francisco `Email` = john.doe@elitesports.com `Phone` = 1-415-555-1234	san francisco john.doe@elitesports.com san francisco 1-415-555-1234

3. **Match key values for the new record are compared with those from existing records.**

Table 10: Existing Records Compared with New Record

Record	Matching Field Values	Match Key Values	Match?
1	`City` = San Frncisco `Email` = john.doe@elitesports.com `Phone` = 1-415-555-1234	san frnciscojohn.doe@elitesports.com san frncisco1-415-555-1234	No. Not considered a duplicate.

Record	Matching Field Values	Match Key Values	Match?
2	`City` = San Francisco `Email` = john.doe@elitesports.com `Phone` = 1-415-555-1111	san franciscojohn.doe@elitesports.com san francisco1-415-555-1111	Yes. The first match key values are identical, so the record is considered a potential duplicate. Only one match key value match is needed.

4. **Determine if the new record is a potential duplicate.** Does the new record have the same match key value as an existing record?
   - Yes—The new record is considered a potential duplicate. It's evaluated further using other matching resources, including matching algorithms.
   - No—The new record is not considered a duplicate.

Duplicate Rule Reference

Here's some additional information that will help you understand how duplicate rules work and how to use them.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

IN THIS SECTION:

Standard Duplicate Rules

Starting in Spring '15, new Salesforce orgs come with standard account, contact, and lead duplicate rules already set up and activated. These rules define what happens when you try to save a duplicate record. Each standard duplicate rule has a corresponding standard matching rule that determines how two records are identified as duplicates.

Standard Duplicate Rules

Starting in Spring '15, new Salesforce orgs come with standard account, contact, and lead duplicate rules already set up and activated. These rules define what happens when you try to save a duplicate record. Each standard duplicate rule has a corresponding standard matching rule that determines how two records are identified as duplicates.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

IN THIS SECTION:

Standard Account Duplicate Rule

Like all duplicate rules, the standard duplicate rule used for account records defines what happens when you try to save a duplicate record. If you try to save a new account, an alert is shown.

Standard Contact Duplicate Rule

Like all duplicate rules, the standard duplicate rule used for contact records defines what happens when you try to save a duplicate record. If you try to save a new contact, an alert is shown.

Standard Lead Duplicate Rule

Like all duplicate rules, the standard duplicate rule used for lead records defines what happens when you try to save a duplicate record. If you try to save a new lead, an alert is shown.

Standard Account Duplicate Rule

Like all duplicate rules, the standard duplicate rule used for account records defines what happens when you try to save a duplicate record. If you try to save a new account, an alert is shown.

Rule Details

Rule Name	Standard Account Duplicate Rule
Description	Duplicate rule for account records
Object	Account
Record-Level Security	Enforce Sharing Rules

Actions

Actions specify what happens when you try to save a duplicate record.

Action On Create	Allow: Alert and Report
Action On Edit	Allow: Report
Alert Text	Duplicate Alert

Matching Rules

Matching rules define how duplicates are identified. At least 1 matching rule must be specified for a duplicate rule.

Compare Account With	Accounts
Matching Rule	Standard Account Matching Rule
Matching Criteria	Matching rule for account records
Field Mapping	Mapping Selected

Standard Contact Duplicate Rule

Like all duplicate rules, the standard duplicate rule used for contact records defines what happens when you try to save a duplicate record. If you try to save a new contact, an alert is shown.

Rule Details

Rule Name	Standard Contact Duplicate Rule
Description	Duplicate rule for contact records
Object	Contact
Record-Level Security	Enforce Sharing Rules

Actions

Actions specify what happens when you try to save a duplicate record.

Action On Create	`Allow: Alert and Report`
Action On Edit	`Allow: Report`
Alert Text	`Duplicate Alert`

Matching Rules

Matching rules define how duplicates are identified. At least 1 matching rule must be specified for a duplicate rule.

Compare Account With	`Contacts`
Matching Rule	`Standard Contact Matching Rule`
Matching Criteria	`Matching rule for contact records`
Field Mapping	`Mapping Selected`

Standard Lead Duplicate Rule

Like all duplicate rules, the standard duplicate rule used for lead records defines what happens when you try to save a duplicate record. If you try to save a new lead, an alert is shown.

Rule Details

Rule Name	`Standard Lead Duplicate Rule`
Description	`Duplicate Rule for Lead Records`
Object	`Lead`
Record-Level Security	`Enforce Sharing Rules`

Actions

Actions specify what happens when you try to save a duplicate record.

Action On Create	`Allow: Alert and Report`
Action On Edit	`Allow: Report`
Alert Text	`Duplicate Alert`

Matching Rules

Matching rules define how duplicates are identified. At least 1 matching rule must be specified for a duplicate rule.

Compare Account With	`Leads`
Matching Rule	`Standard Lead Matching Rule`
Matching Criteria	`Matching rule for lead records`
Field Mapping	`Mapping Selected`

Duplicate Management FAQs

Answers to common questions about Data.com Duplicate Management.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

IN THIS SECTION:

How does duplicate prevention work with Data.com Prospector and Data.com Clean?

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

Adding Records with Data.com Prospector

It depends on what your organization's Data.com duplicate preferences are.

If your organization does not allow duplicate records to be added to Salesforce from Data.com, then Data.com will block duplicate records from being added to Salesforce and the duplicate rule won't need to run. The user trying to add records from Data.com will receive an error log detailing which records couldn't be added because they are duplicates.

If your organization allows duplicate records to be added to Salesforce from Data.com, then the duplicate rules will run. The duplicate rule will determine if the duplicate record is allowed or blocked. Records that are blocked by the duplicate rule will appear in the error log.

Updating Records with Data.com Clean

It depends on what your organization's duplicate rules are. If your duplicate rule is set to block duplicates on edit, then a record can't be cleaned if cleaning creates a duplicate.

For Clean jobs, if your duplicate rule is set to block or alert, then a record can't be cleaned if the cleaning creates a duplicate. An entity error appears in the Clean Jobs History table for any record that can't be cleaned during a job.

If your duplicate rule is set to allow duplicates on edit, then a record can be cleaned even if it creates a duplicate. In addition, no alert displays when manually cleaning records even if your duplicate rule is set to alert.

Why am I getting an error saying my matching rule uses too many OR operators within groupings?

A matching rule has a limit of 10 fields that are arranged into an equation. When a matching rule is saved, we rewrite the equation into a standardized format that translates the OR statements to AND statements. The standardized format has a limit of 10 rows.

Example: If your matching rule includes the following equation...

(Field 1 OR Field 2) AND

(Field 3 OR Field 4) AND

(Field 5 OR Field 6) AND

(Field 7 OR Field 8)

...it would be rewritten as

(Field 1 AND Field 3 AND Field 5 Field AND 7) OR

(Field 1 AND Field 3 AND Field 5 AND Field 8) OR

(Field 1 AND Field 3 AND Field 6 AND Field 7) OR

(Field 1 AND Field 3 AND Field 6 AND Field 8) OR

(Field 1 AND Field 4 AND Field 5 AND Field 7) OR

(Field 1 AND Field 4 AND Field 5 AND Field 8) OR

(Field 1 AND Field 4 AND Field 6 AND Field 7) OR

(Field 1 AND Field 4 AND Field 6 AND Field 8) OR

(Field 2 AND Field 3 AND Field 5 AND Field 7) OR

(Field 2 AND Field 3 AND Field 5 AND Field 8) OR

(Field 2 AND Field 3 AND Field 6 AND Field 7) OR

(Field 2 AND Field 3 AND Field 6 AND Field 8)OR

(Field 2 AND Field 4 AND Field 5 AND Field 7) OR

(Field 2 AND Field 4 AND Field 5 AND Field 8) OR

(Field 2 AND Field 4 AND Field 6 AND Field 7) OR

(Field 2 AND Field 4 AND Field 6 AND Field 8)

Although this matching rule is within the field limit, it exceeds the row limit of 10 when written in the standardized format, and therefore can't be saved. You need to refine the matching rule so it uses fewer OR operators within groupings.

SEE ALSO:

Match Keys Used with Matching Rules

Security

Salesforce is built with security 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

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. Your data is protected from unauthorized access from outside your company. Also safeguard it from inappropriate usage by your users.

IN THIS SECTION:

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 you should refuse to 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 will continue 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 will allow 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 529.
- Set session security restrictions to make spoofing more difficult. For more information, see Modify Session Security Settings on page 540.
- Educate your employees not to open suspect emails and to be vigilant in guarding against phishing attempts.
- Use security solutions from leading vendors such as Symantec 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, such as RSA tokens, to restrict access to your network. For more information, see Two-Factor Authentication on page 518.
- Use Transaction Security to monitor events and take appropriate actions. For more information, see Transaction Security Policies on page 556.

Salesforce has a Security Incident Response Team to respond to any security issues. To report a security incident or vulnerability to Salesforce, please contact security@salesforce.com. Describe the issue in detail, and the team will respond promptly.

Security Infrastructure

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.

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.

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

Health Check lets you identify and fix security vulnerabilities in your password policies, network access configuration, and session settings, all from a single page. A summary score shows how your org measures against the Salesforce-recommended baseline.

From Setup, enter *Health Check* in the Quick Find box, then select **Health Check**.

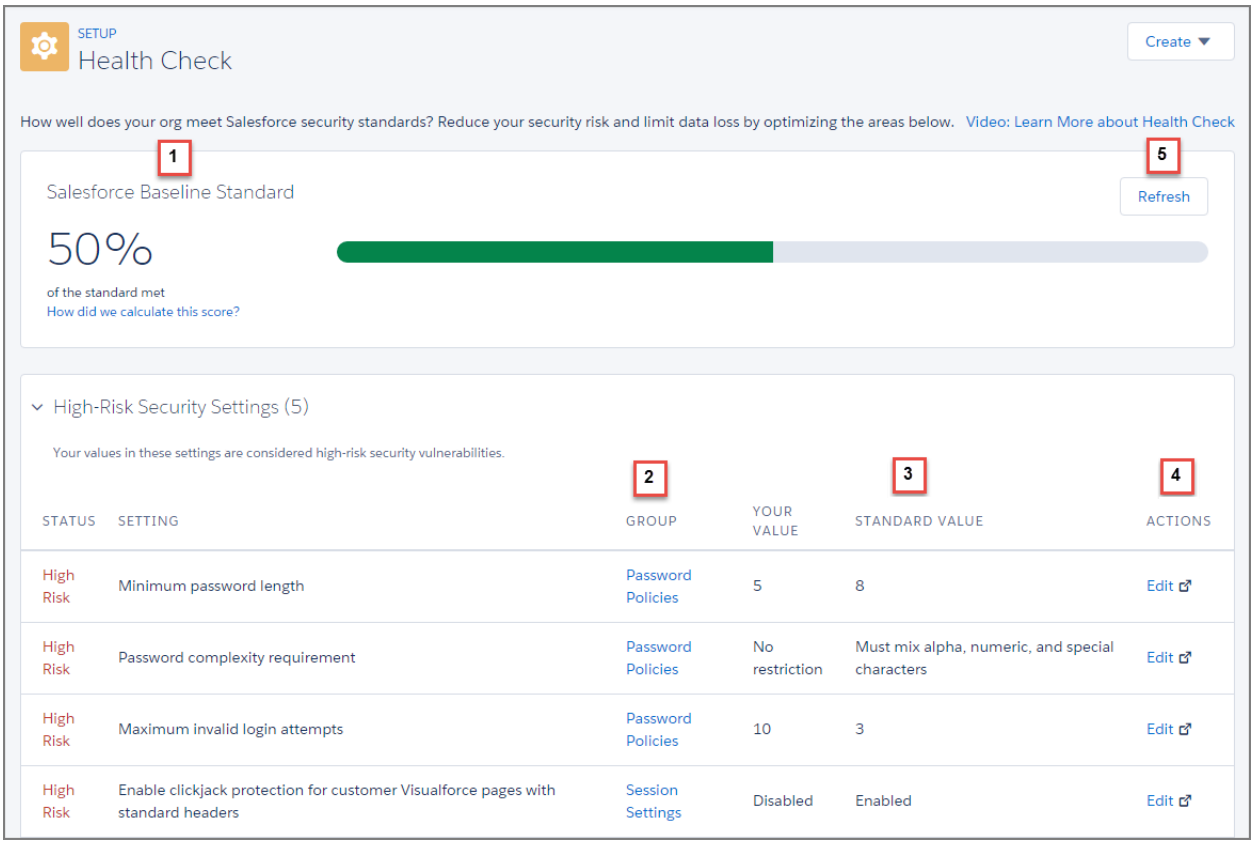
The Salesforce Baseline standard (1) is a set of recommended values for Session Settings, Password Policies, and Network Access setting groups (2). If you change all of a group's settings to be less restrictive than what's in the Salesforce Baseline standard, your health check score decreases.

Your high- and medium-risk settings are shown with information about how they compare against the standard value (3). To remediate a risk, edit the setting (4) and refresh your score (5) to see whether it improved. Your settings that meet the standard are listed at the bottom.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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



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.

IN THIS SECTION:

How Is the Health Check Score Calculated?

The Health Check total score is calculated by a proprietary formula that assigns an internal score to the Password Policies, Session Settings, and Network Access setting groups. Each group's score reflects how well all of the settings in that group meet the Salesforce Baseline standard. Groups with all settings that meet or exceed the standard get the highest possible score, and groups containing settings at high risk get the lowest score. Also, some settings have a heavier weight. Group scores are used in the proprietary formula to calculate your total score.

SEE ALSO:

How Is the Health Check Score Calculated?

Security Implementation Guide

How Is the Health Check Score Calculated?

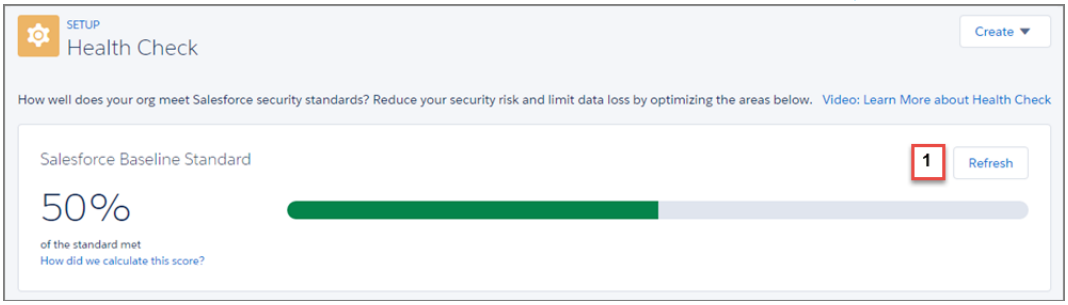
The Health Check total score is calculated by a proprietary formula that assigns an internal score to the Password Policies, Session Settings, and Network Access setting groups. Each group's score reflects how well all of the settings in that group meet the Salesforce Baseline standard. Groups with all settings that meet or exceed the standard get the highest possible score, and groups containing settings at high risk get the lowest score. Also, some settings have a heavier weight. Group scores are used in the proprietary formula to calculate your total score.

If all of the settings in your setting groups meet or exceed the standard, your total score is 100%. As you update your settings, refresh health check (1) to see how the updates affect your total score. Hopefully 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



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 remediating high risks in your Password Policies and other setting groups.

The Salesforce Baseline Standard

Following are the setting values that meet the standard, are considered medium risk, and are considered high risk.

Password Policies

Setting	Standard Value	Medium-Risk Value	High-Risk Value
`User passwords expire in`	90 days or less	180 days	One year or Never expires
`Enforce password history`	3 or more passwords remembered	1 or 2 passwords remembered	No passwords remembered

Setting	Standard Value	Medium-Risk Value	High-Risk Value
`Minimum password length` (see Note)	8	6 or 7	5 or less
`Password complexity requirement` (see Note)	Must mix alpha, numeric, and special characters, or more complex	Must mix alpha and numeric characters	No restriction
`Password question requirement`	Cannot contain password	None	N/A
`Maximum invalid login attempts`	3	5	10 or No Limit
`Lockout effective period`	15 minutes	30 or 60 minutes	Forever (must be reset by admin)
`Obscure secret answer for password resets`	Checkbox selected	Checkbox deselected	N/A
`Require a minimum 1 day password lifetime`	Checkbox selected	Checkbox deselected	N/A

Note: The `Minimum password length` and `Password complexity requirement` settings count twice as much as other settings in the calculation of your Password Policies group score.

Network Access

Setting	Standard Value	Medium Risk Value	High Risk Value
`Trusted IP Ranges`	1 or more ranges set	No range set	N/A

Session Settings

Setting	Standard Value	Medium Risk Value	High Risk Value
`Timeout Value`	2 hours or less	4, 8, or 12 hours	N/A
`Disable session timeout warning popup`	Checkbox selected	Checkbox deselected	N/A
`Force logout on session timeout`	Checkbox selected	Checkbox deselected	N/A
`Lock sessions to the IP address from which they originated` (see Note)	Checkbox selected	Checkbox deselected	N/A
`Lock sessions to the domain in which they were first used`	Checkbox selected	N/A	Checkbox deselected
`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

Setting	Standard Value	Medium Risk Value	High Risk Value
Enable caching and autocomplete on login page	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 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

Note: This setting is available in **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions.

SEE ALSO:

Security Health Check

Auditing

Auditing features don't secure your organization by themselves; they provide information about usage of the system, which can be critical in diagnosing potential or real security issues. 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 694.

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 Track Field History on page 705.

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 702.

Platform Encryption

Platform Encryption gives your data a whole new layer of security while preserving critical platform functionality. The data you select is encrypted at rest using an advanced key derivation system. You can protect data at a more granular level than ever before, so that your company can confidently comply with privacy policies, regulatory requirements, and contractual obligations for handling private data.

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

IN THIS SECTION:

Encrypt Fields and Files

To implement Platform Encryption in your organization, create a tenant secret and then specify the fields and files you want to encrypt, and designate users who can generate, rotate and archive your organization's keys.

Set Up Platform Encryption

With Platform Encryption, you manage your own tenant secret, which is used to derive the encryption keys that protect your data. Keys are never saved or shared across organizations. Instead, they are derived on demand from a master secret and an organization-specific tenant secret and then cached on an application server.

How Platform Encryption Works

Platform Encryption builds on the data encryption options that Salesforce offers out of the box. It enables you to encrypt the data stored in many standard and custom fields and in files and attachments. Data is encrypted at rest, not just when transmitted over a network, so it is protected even when other lines of defense have been compromised.

SEE ALSO:

Salesforce Platform Encryption Implementation Guide

Encrypt Fields and Files

To implement Platform Encryption in your organization, create a tenant secret and then specify the fields and files you want to encrypt, and designate users who can generate, rotate and archive your organization's keys.

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

IN THIS SECTION:

Encrypt Fields

Select the fields you want to encrypt. When a field is encrypted, its value appears as asterisks to users who don't have permission to view it.

Encrypt Files and Attachments

For another layer of data protection, encrypt files and attachments using Platform Encryption. When Platform Encryption is on, the body of each file or attachment is encrypted when it's uploaded.

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 your tenant secret and keys are backed up, and be careful who you allow to manage your secrets and keys.

Encrypt Fields

Select the fields you want to encrypt. When a field is encrypted, its value appears as asterisks to users who don't have permission to view it.

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, enter *Platform Encryption* in the Quick Find box, then select **Platform Encryption**.
3. Select **Encrypt Fields**.
4. Select **Edit**.
5. Select the fields to encrypt, and save your settings.

The automatic Platform Encryption validation service kicks off. If any of your organization's settings are blocking encryption, you will receive an email with instructions for fixing them.

Field values are automatically encrypted only in records created or updated after you've enabled encryption. Salesforce recommends updating existing records to ensure that their field values are encrypted. For example, if you encrypt the Description field on the Case object, use the Data Loader to update all case records. Contact Salesforce if you need help with this.

Note: This information applies to Platform Encryption and not to Classic Encryption.

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

USER PERMISSIONS

To view setup:
- "View Setup and Configuration"

To encrypt fields:
- "Customize Application"

SEE ALSO:

Which Fields Can I Encrypt?

Platform Encryption Field Limits

Data Loader

Back to Parent Topic

Encrypt Files and Attachments

For another layer of data protection, encrypt files and attachments using Platform Encryption. When 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.

You can encrypt these kinds of files:

- Files attached to feeds
- Files attached to records
- Files on the Content, Libraries, and Files tabs (Salesforce Files, including file previews, and Salesforce CRM Content files)
- Files managed with Salesforce Files Sync
- Files attached to Chatter posts, comments, and the sidebar
- Notes

Some types of files and attachments can't be encrypted:

- Chatter group photos
- Chatter profile photos
- Documents

1. From Setup, enter *Platform Encryption* in the Quick Find box, then select **Platform Encryption**.
2. Select **Encrypt Files and Attachments**.
3. Click **Set Preferences**.

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 add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

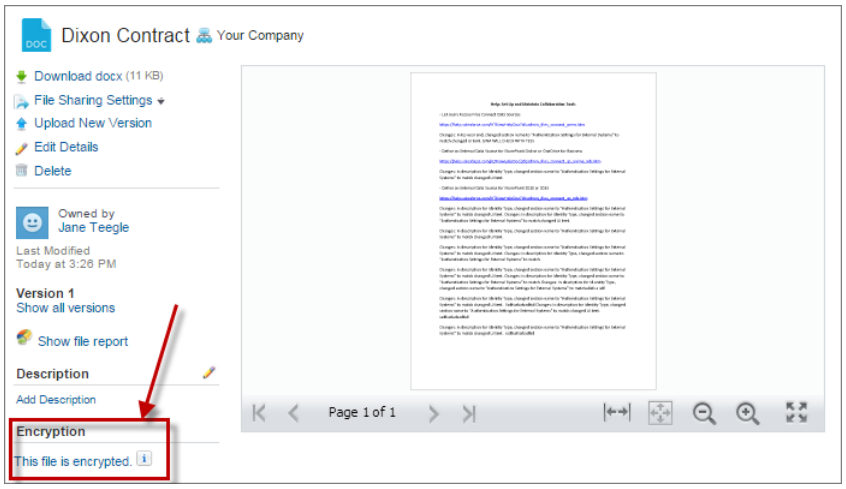
Available in Salesforce Classic.

USER PERMISSIONS

To view setup:
- "View Setup and Configuration"

To encrypt files:
- "Customize Application"

Here's what it looks like when a file is encrypted.



Note: This information applies to Platform Encryption and not to Classic Encryption.

SEE ALSO:

Back to Parent Topic

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 your tenant secret and keys are backed up, and be careful who you allow to manage your secrets and keys.

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

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.
   - 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 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. Understand that encryption applies to all users, regardless of their permissions.

- You control who reads encrypted field values in plaintext using the "View Encrypted Data" permission. However, the data stored in these fields is encrypted at rest, regardless of user permissions.
- Functional limitations are imposed on users who interact with encrypted data. Consider whether encryption can be applied to a portion of your business users and how this application affects other users interacting with the data.

5. Read the Platform Encryption considerations and understand their implications on your organization.
   - Evaluate the impact of the considerations on your business solution and implementation.
   - Test 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.
6. 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 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 Platform Encryption.
   - Apps on the AppExchange that are built exclusively using Force.com inherit Platform Encryption capabilities and limitations.
7. 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. Make sure that a user inadvertently granted the View Encrypted Data permission would still see only appropriate data.

   By default, any user can edit encrypted fields, even users without the "View Encrypted Data" permission.
8. 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.
9. Grant the "View Encrypted Data" user permission to authorized users only.

   Grant the "View Encrypted Data" permission to users who must view encrypted fields in plaintext, including integration users who must read sensitive data in plaintext. Encrypted files are visible to all users who have access to the files, regardless of the "View Encrypted Data" permission.
10. Mass-encrypt your existing data.

    Existing field and file data is not automatically encrypted when you turn on 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.
11. Avoid encrypting Currency, Number, Date, and Date/Time data.

    You can often keep private, sensitive, or regulated data safe without encrypting associated `Currency`, `Number`, `Date`, and `Date/Time` fields. Encrypting these fields can have broad functional consequences across the platform, such as disruptions to roll-up summary reports, report timeframes, and calculations.
12. Communicate to your users about the impact of encryption.

    Before you enable Platform Encryption in a production environment, inform users about how it affects your business solution. For example, share the information described in Platform Encryption considerations, where it's relevant to your business processes.

13. Use discretion when granting login access.

If a user with the "View Encrypted Data" permission grants login access to another user, the other user is able to view encrypted fields in plaintext.

14. 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

Set Up Platform Encryption

With Platform Encryption, you manage your own tenant secret, which is used to derive the encryption keys that protect your data. Keys are never saved or shared across organizations. Instead, they are derived on demand from a master secret and an organization-specific tenant secret and then cached on an application server.

After you create a unique tenant secret for your organization, you can rotate it, archive it, and share responsibility for it with other users.

Developers can generate tenant secrets by coding a call to the TenantSecret object in the Salesforce API.

Important: Only authorized users can generate tenant secrets from the Platform Encryption page. Ask your Salesforce administrator to assign you the "Manage Encryption Keys" permission.

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

USER PERMISSIONS

To manage tenant secrets:

- "Manage Encryption Keys"

IN THIS SECTION:

Create a Tenant Secret

Create a unique tenant secret for your organization, then authorize specific people to use it to produce new data encryption keys.

Rotate Your Platform Encryption Keys

You should regularly generate a new tenant secret and archive the previously active one. By controlling the lifecycle of your organization's tenant secrets, you control the lifecycle of the derived data encryption keys.

Export and Import a 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 Platform Encryption Off

At some point you may need to disable 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:

Which User Permissions Does Platform Encryption Require?

The TenantSecret Object

Back to Parent Topic

Create a Tenant Secret

Create a unique tenant secret for your organization, then authorize specific people to use it to produce new data encryption keys.

1. Assign the "Manage Encryption Keys" permission to people you trust to manage tenant secrets for your organization.

   You can add this permission to a profile or a permission set: from Setup, enter *Profiles* or *Permission Sets* in the Quick Find box.

2. Create your tenant secret.

   a. From Setup, enter *Platform Encryption* in the Quick Find box, then select **Platform Encryption**.

   b. Click **Create Tenant Secret**.

Note: This information applies to Platform Encryption and not to Classic Encryption.

SEE ALSO:

Permission Sets

Profiles

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

USER PERMISSIONS

To manage tenant secrets:

- "Manage Encryption Keys"

Rotate Your Platform Encryption Keys

You should regularly generate a new tenant secret and archive the previously active one. By controlling the lifecycle of your organization's tenant secrets, you control the lifecycle of the derived data encryption keys.

Your key rotation is determined by your organization's security policies. You can rotate the tenant secret once every 24 hours in a production organization, and every four hours in a sandbox environment. Master secrets used in the key derivation function are rotated with each major Salesforce release. This has no impact on the customer keys or on encrypted data, until the tenant secret is rotated.

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

USER PERMISSIONS

To manage tenant secrets:
- "Manage Encryption Keys"

1. Check the statuses of keys in your organization from Setup by entering *Platform Encryption* in the Quick Find box, then selecting **Platform Encryption**. Keys can be active, archived, or destroyed.

   ACTIVE
   Can be used to encrypt and decrypt new or existing data.

   ARCHIVED
   Cannot encrypt new data. Can be used to decrypt data previously encrypted with this key when it was active.

   DESTROYED
   Cannot encrypt or decrypt data. Data encrypted with this key when it was active can no longer be decrypted.

2. From Setup, enter *Platform Encryption* in the Quick Find box, then select **Platform Encryption**.
3. Click **Generate New Tenant Secret**.
4. If you want to re-encrypt existing field values with a newly generated tenant secret, edit and save the encrypted fields using the Data Loader or another tool.

   Get the data to update by exporting the objects via the API or by running a report that includes the record ID. This triggers the encryption service to encrypt the existing data again using the newest key.

Note: This information applies to Platform Encryption and not to Classic Encryption.

Export and Import a 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. From Setup, enter *Platform Encryption* in the Quick Find box, then select **Platform Encryption**.
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 information applies to Platform Encryption and not to Classic Encryption.

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

USER PERMISSIONS

To manage tenant secrets:
- "Manage Encryption Keys"

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

1. From Setup, enter *Platform Encryption* in the Quick Find box, then select **Platform Encryption**.
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.

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.

Note: This information applies to Platform Encryption and not to Classic Encryption.

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

USER PERMISSIONS

To manage tenant secrets:
- "Manage Encryption Keys"

Turn Platform Encryption Off

At some point you may need to disable 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 Platform Encryption, encrypted data is not mass-decrypted and any functionality that is affected by encryption is not restored. Contact Salesforce if you need help with this.

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**.
   Data in these fields will now be visible to users without the "View Encrypted Data" permission, if they have access.
4. To disable encryption for files, deselect **Encrypt Files and Attachments**.
   All files and attachments will now be visible to users without the "View Encrypted Data" permission, if they have access.

The limitations and special behaviors that apply to encrypted fields persist after encryption is disabled. The values can remain encrypted at rest and masked in some places. All previously encrypted files and attachments 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.

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

USER PERMISSIONS

To view setup:
- "View Setup and Configuration"

To disable encryption:
- "Customize Application"

SEE ALSO:

Back to Parent Topic

How Platform Encryption Works

Platform Encryption builds on the data encryption options that Salesforce offers out of the box. It enables you to encrypt the data stored in many standard and custom fields and in files and attachments. Data is encrypted at rest, not just when transmitted over a network, so it is protected even when other lines of defense have been compromised.

Encrypting files, fields, and attachments has no effect on your organization's storage limits.

Note: This information applies to Platform Encryption and not to Classic Encryption.

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

IN THIS SECTION:

Behind the Scenes: The Platform Encryption Process

When users submit data, the application server looks for the organization-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.

Automatic Validation for Platform Encryption

When you turn on encryption, Salesforce automatically checks for potential side effects and warns you if any existing settings may pose a risk to data access or the normal operation of your Salesforce organization. For example, encryption is blocked if you try to encrypt fields used in criteria-based sharing rules.

Which User Permissions Does Platform Encryption Require?

Assign permissions to your users according to their roles with regard to encryption. Some users will need the "View Encrypted Data" permission. Some will need other combinations of permissions in order to select data for encryption or work with encryption keys.

Platform Encryption Data Visibility

Users and administrators see information based on a combination of factors described here. However, you control who has access to sensitive data.

How Do I Deploy Platform Encryption?

When you deploy 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 Platform Encryption is enabled in the target organization.

How Does Platform Encryption Work In a Sandbox?

Refreshing a sandbox from a production organization creates an exact copy of the production organization. If Platform Encryption is enabled on the production organization, all encryption settings are copied, including tenant secrets created in production.

What's the Difference Between Classic Encryption and Platform Encryption?

Classic encryption lets you protect a special type of custom text fields, which you create for that purpose. With Platform Encryption you can encrypt a variety of widely-used standard fields, along with some custom fields and many kinds of files. Platform Encryption also supports person accounts, cases, search, workflow, approval processes, and other key Salesforce features.

Limitations and Considerations for Platform Encryption

Understand the possible results of platform encryption before you enable it to improve data protection in your organization.

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

IN THIS SECTION:

Some Apps Don't Work with Encrypted Data

Some Salesforce feature sets don't work with data that's encrypted at rest.

Platform Encryption Field Limits

Under certain conditions, encrypting a given field can impose limits on the values you store in that field. Before deciding to encrypt a field, make sure you know what functionality will be affected.

General Platform Encryption Considerations

These considerations apply to all data that you encrypt using Platform Encryption.

Some Apps Don't Work with Encrypted Data

Some Salesforce feature sets don't work with data that's encrypted at rest.

These apps don't support data that's encrypted at rest. Check this page for changes to the list of unsupported apps.

- Chatter Desktop
- Connect Offline
- Data.com
- ExactTarget
- Exchange Sync
- Flows
- Legacy portals: customer, self-service, and partner
- Lightning Components
- Organization Sync
- Pardot
- Process Builder
- Salesforce App for Outlook
- Salesforce Classic Mobile
- Salesforce for Outlook
- Salesforce IQ
- Salesforce to Salesforce
- Visual Workflows
- Wave
- Work.com

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

Other Apps

Some apps are supported, but with caveats.

- 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 information applies to Platform Encryption and not to Classic Encryption.

SEE ALSO:

Back to Parent Topic

Platform Encryption Field Limits

Under certain conditions, encrypting a given field can impose limits on the values you store in that field. Before deciding to encrypt a field, make sure you know what functionality will be affected.

If you expect users to enter non-ASCII values, we recommend creating validation rules to enforce these limits:

- Email custom field values that contain only non-ASCII characters are limited to 70 characters.
- Phone custom fields values that contain only non-ASCII characters are limited to 22 characters.

Note: This information applies to Platform Encryption and not to Classic Encryption.

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

SEE ALSO:

Back to Parent Topic

General Platform Encryption Considerations

These considerations apply to all data that you encrypt using Platform Encryption.

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

Search

- Search index files are not encrypted.
- 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.

SOQL/SOSL

- If you query encrypted data, invalid strings return an `INVALID_FIELD` error instead of the expected `MALFORMED_QUERY`.
- 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 SOQL/WHERE clauses with SOSL/FIND queries. For example, SOQL/WHERE won't work with encrypted fields in computer-telephony integration (CTI).

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.

Salutation and Suffix field values in Contact records can appear masked to users without the “View Encrypted Data” permission, even if the field values aren’t encrypted.

Field Audit Trail

If your organization has Field Audit Trail enabled, previously archived data isn't encrypted when you turn on Platform Encryption. 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 are encrypted as they are created, and 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 continues to be stored without encryption. If your organization needs to encrypt previously archived data, contact Salesforce.

Page Layouts

If you preview a page layout as a profile without the “View Encrypted Data” permission, the preview's sample data isn’t masked. Instead, the sample data may be blank or appear in plaintext.

Email

- When encrypted field values are included in email templates, they appear in plaintext to users with the “View Encrypted Data” permission. Otherwise, whether the recipient sees plaintext or masked data is determined by the running user's permissions.
- Users without the “View Encrypted Data” permission can’t send Stay-in-Touch requests.
- Users without the “View Encrypted Data” permission can’t send emails using Mass Email Contacts.
- When the standard Email field is encrypted, Email to Salesforce can't receive inbound emails.

Communities

For community users with the "View Encrypted Data" permission, data encryption doesn't change anything about the community experience. However, 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`.

Activities

- When the Contact Name field is encrypted, Shared Activities lookup is not supported.
- When an Activity History related list contains references to encrypted fields, those fields are encrypted in their original context. The list itself is not encrypted, and any unencrypted values in the list are visible in plaintext.

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 on disk unencrypted.
- You can't aggregate, sort, or filter on encrypted data.

Exact Target

When the Exact Target connector is installed, the Account Name field can't be encrypted. If the Account Name field is encrypted, the Exact Target connecter can't be installed.

Campaigns

Campaign member search isn't supported when you search by encrypted fields.

General

- Encrypted fields can't be used in:
  - Criteria-based sharing rules.
  - Similar opportunities searches.
  - External lookup relationships.
  - Skinny tables.
  - Filter criteria for data management tools.
  - Duplicate Management matching rules.
- In the Salesforce1 mobile app, records cloned by users without the "View Encrypted Data" permission show masked data for encrypted fields.
- Live Agent chat transcripts are not encrypted at rest.
- Live Agent chat transcripts are not encrypted at rest.

Note: This information applies to Platform Encryption and not to Classic Encryption.

SEE ALSO:

Back to Parent Topic

Which Fields Can I Encrypt?

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

You can encrypt certain fields on the Account, Contact, Case, and Case Comment objects. When Platform Encryption is on, users with the "View Encrypted Data" permission can see the contents of encrypted fields, but users without that permission see only masked values (that is, the values are replaced with asterisks).

In either case, encrypted fields work normally throughout the Salesforce user interface, business processes, and APIs. (There are some exceptions; for example, encrypted fields can't be sorted.)

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.

Encrypted Standard Fields

You can encrypt the contents of these standard field types.

- On the Account object:
  - `Account Name`
  - `Fax`
  - `Website`
  - `Phone`
- On the Contact object:
  - `Description`
  - `Email`
  - `Fax`
  - `Home Phone`
  - `Mailing Address` (Encrypts only `Mailing Street` and `Mailing City`)
  - `Mobile`
  - `Name` (Encrypts `First Name`, `Middle Name`, and `Last Name`)
  - `Other Phone`
  - `Phone`
- On the Case object:
  - `Subject`
  - `Description`
- On Case Comments:
  - `Body`

Encrypted Custom Fields

You can encrypt the contents of these custom field types:

- Email
- Phone
- Text
- Text Area
- Text Area (Long)
- URL

Important: Once 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.

You can't use currently or previously encrypted custom fields in custom formula fields or criteria-based sharing rules.

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 that are used in custom formula fields
- Fields on external data objects

Note: This information applies to Platform Encryption and not to Classic Encryption.

SEE ALSO:

Back to Parent Topic

Platform Encryption Terminology

Encryption has its own specialized vocabulary. To get the most out of your 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 add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

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
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. 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. 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 Platform Encryption Process

When users submit data, the application server looks for the organization-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 add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

Platform Encryption Process Flow

1. 1. When a Salesforce user saves encrypted data, the runtime engine determines from metadata whether the field, file, or attachment should be encrypted before storing it in the database.
2. 2. If so, the encryption service checks for the matching data encryption key in cached memory.
3. 3. The encryption service determines if the key exists.
   a. If so, the encryption service retrieves the key.
   b. Otherwise, the service sends a derivation request to a key derivation server and returns it to the encryption service running on the App Cloud.
4. 4. After retrieving or deriving the key, the encryption service generates a random initialization vector (IV) and encrypts the data using JCE's AES-256 implementation.
5. 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

Automatic Validation for Platform Encryption

When you turn on encryption, Salesforce automatically checks for potential side effects and warns you if any existing settings may pose a risk to data access or the normal operation of your Salesforce organization. For example, encryption is blocked if you try to encrypt fields used in criteria-based sharing rules.

Validation results are returned via email when you use the UI and are synchronous when you use the API.

If the validation process gives you an error message when you enable Platform Encryption, you may be able to use this information to solve the issue. These are the factors that the validation service checks:

Criteria-Based Sharing Rules
Fields can't be used in criteria-based sharing rules.

SOQL queries
Encrypted fields cannot be used in certain portions of a SOQL query.

Formula fields
Formula fields cannot reference encrypted fields.

Skinny tables
Fields used in skinny tables cannot be encrypted, and encrypted fields cannot be used in skinny tables.

Portals
If legacy portals are enabled in your organization, you can't encrypt standard fields. If you encrypt standard fields, you can't enable legacy portals. Deactivate all portals to enable encryption on standard fields.

Email Plugins
If Exchange Sync or Salesforce App for Oultook is activated, Platform Encryption can't be enabled. If Salesforce for Outlook is activated, Platform Encryption can be enabled, but Salesforce for Outlook stops working. If Platform Encryption is enabled, none of the three plugins can be activated.

Note: This information applies to Platform Encryption and not to Classic Encryption.

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

SEE ALSO:

Encrypt Fields
Encrypt Files and Attachments
Back to Parent Topic

Which User Permissions Does Platform Encryption Require?

Assign permissions to your users according to their roles with regard to encryption. Some users will need the "View Encrypted Data" permission. Some will need other combinations of permissions in order to select data for encryption or work with encryption keys.

	View Encrypted Data	Manage Encryption Keys	Customize Application	View Setup and Configuration
View data in encrypted fields	✔			
View Platform Encryption setup page			✔	✔
Edit Platform Encryption setup Page, excluding key management			✔	
Generate, destroy, export, and import tenant secrets		✔		
Query TenantSecret object via the API		✔		

The "View Encrypted Data" Permission

As administrator, you decide which users can see field values unmasked. You do this by granting the "View Encrypted Data" permission in profiles or permission sets. Administrators do not automatically have the permission, and standard profiles do not include it by default.

Tip:

When you have the "View Encrypted Data" permission and grant login access to other users, they can see encrypted field values in plain text. To avoid exposing sensitive data, clone your profile, remove the "View Encrypted Data" permission from the cloned profile, and assign yourself to the cloned profile; then grant login access to the other user.

When you turn encryption on, existing field values aren't encrypted immediately. Values are encrypted only after they are touched.

An encrypted file is visible to all users who have access to that file, regardless of the "View Encrypted Data" permission.

Users without the "View Encrypted Data" permission can't:

- Edit required encrypted lookup fields.
- Use Chatter publisher related lists,
- Use the Copy Mailing Address to Other Address functionality in contacts.
- Choose which value to keep from two merged account records if the same value is encrypted in both. When this happens, Salesforce retains the value from the master account record.
- Create records that require a value for an encrypted standard field.

When the running user on a report or dashboard has the View Encrypted Data permission, readers of the report chart or dashboard who don't have the View Encrypted Data permission may still see encrypted data.

When users without the "View Encrypted Data" permission clone a record with encrypted, non-lookup fields, the encrypted field values are blank in the new record.

When a user who doesn't have the "View Encrypted Data" permission clones a record, encrypted fields show masked data.

Users without the "View Encrypted Data" permission can still do some things with encrypted fields:

- Change the value of an encrypted field, unless the field-level security is set to read-only.
- See encrypted fields in search results, although their values are masked.
- Create contact and opportunity records from Chatter actions, related lists on account detail pages, and Quick Create.

Note: This information applies to Platform Encryption and not to Classic Encryption.

SEE ALSO:

- Profiles
- Permission Sets
- Platform Encryption Data Visibility
- Back to Parent Topic

Platform Encryption Data Visibility

Users and administrators see information based on a combination of factors described here. However, you control who has access to sensitive data.

When users work in an organization with Platform Encryption enabled, it's important that they understand the difference between encrypted data at rest and data masking. Encrypted data at rest refers to data encrypted when stored. Masking refers to hiding visible data in a field by replacing the characters.

Users *can* view, depending on permissions or whether the data resides in a file or field, some data in cleartext instead of as masked. There are a couple of reasons for this behavior:

- Permissions. Users who must access certain, sensitive data can have the View Encrypted Data permission enabled. For example, a human resources director might need to view sensitive employee information in a field, while a clerk doesn't. Although the human resources director can view the sensitive data, it remains encrypted at rest.
- Encrypted files remain visible. Although encrypted, files remain visible to users who have access to them. In contrast, to view encrypted data in fields, a user must have the View Encrypted Data permission. Use appropriate sharing settings if data in a file must remain hidden.

How Do I Deploy Platform Encryption?

When you deploy 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 Platform Encryption is enabled in the target organization.

You can use change sets to deploy Platform Encryption to custom fields. Regardless of how you deploy, Salesforce automatically checks to see if the implementation violates Platform Encryption guidelines.

Important: Custom fields in managed packages cannot be encrypted. If you use managed packages in deployment, the Encrypted field attribute is ignored.

Source Organization	Target Organization	Result
Platform Encryption enabled	Platform Encryption enabled	The source Encrypted field attribute indicates enablement
Platform Encryption enabled	Platform Encryption not enabled	The Encrypted field attribute is ignored
Platform Encryption not enabled	Platform Encryption enabled	The target Encrypted field attribute indicates enablement

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

Note: This information applies to Platform Encryption and not to Classic Encryption.

SEE ALSO:

Back to Parent Topic

How Does Platform Encryption Work In a Sandbox?

Refreshing a sandbox from a production organization creates an exact copy of the production organization. If 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 information applies to Platform Encryption and not to Classic Encryption.

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

SEE ALSO:

Back to Parent Topic

What's the Difference Between Classic Encryption and Platform Encryption?

Classic encryption lets you protect a special type of custom text fields, which you create for that purpose. With Platform Encryption you can encrypt a variety of widely-used standard fields, along with some custom fields and many kinds of files. Platform Encryption also supports person accounts, cases, search, workflow, approval processes, and other key Salesforce features.

Feature	Classic Encryption	Platform Encryption
Pricing	Included in base user license	Additional fee applies
Encryption at Rest	✔	✔
Native Solution (No Hardware or Software Required)	✔	✔
Encryption Algorithm	128-bit Advanced Encryption Standard (AES)	256-bit Advanced Encryption Standard (AES)
HSM-based Key Derivation		✔
"Manage Encryption Keys" Permission		✔
Generate, Export, Import, and Destroy Keys	✔	✔

EDITIONS

Available as add-on subscription in: **Enterprise**, **Performance**, and **Unlimited** Editions. Available in **Developer** Edition at no charge for organizations created in Summer '15 and later.

Available in Salesforce Classic.

Feature	Classic Encryption	Platform Encryption
PCI-DSS L1 Compliance	✔	✔ (for fields only)
Text (Encrypted) Field Type	Dedicated custom field type, limited to 175 characters	
Masking	✔	✔
Mask Types and Characters	✔	
"View Encrypted Data" Permission Required to Read Encrypted Field Values	✔	✔
Email Template Values Respect "View Encrypted Data" Permission		✔
Encrypted Standard Fields		✔
Encrypted Attachments, Files, and Content		✔
Encrypted Custom Fields		✔
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		✔

SEE ALSO:

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 their computer unattended while still logged on. It also limits the risk of internal attacks, such as when one employee tries to use another employee's session.

You can control the session expiration time window for user logins. Session expiration allows you to select a timeout for user sessions. 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 do not respond to this prompt, they are automatically logged out.

Note: When a user closes a browser window or tab they are not automatically logged off from their Salesforce session. Please ensure that your users are aware of this, and that they end all sessions properly by clicking *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, apart from Force.com

sites, which can still be accessed using HTTP. If you ask Salesforce to disable this setting and change the URL from `https://` to `http://`, you can still access the application. However, you should require all sessions to use TLS for added security. See Modify Session Security Settings on page 540.

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 543.

IN THIS SECTION:

SEE ALSO:

Set Trusted IP Ranges for Your Organization

Identity Verification History

Modify Session Security Settings

You can modify session security settings to specify connection type, timeout settings, 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 12 hours even though you can only set it as low as 15 minutes. Select a value between 15 minutes and 12 hours. Choose a shorter timeout period if your organization 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 organization, the user must log in again. Note: Do *not* select Disable session timeout warning popup when enabling this option.
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: **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 option 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 to help prevent unauthorized use of the session ID in another domain. This preference is enabled by default for organizations created with the Spring '15 release or later.
`Require secure connections (HTTPS)`	Determines whether HTTPS is required to log in to or access Salesforce, apart from Force.com sites, which can still be accessed using HTTP. This option is enabled by default for security reasons. Note: The Reset Passwords for Your Users page can only be accessed using HTTPS.
`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 option 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 option 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 is not available.
`Use POST requests for cross-domain sessions`	Sets the organization 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"/>` 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 option is enabled, login IP ranges are enforced on each page request, including requests from client applications. If this option is not enabled, login IP ranges are enforced only when a user logs in. This option affects all user profiles that have login IP restrictions.

Field	Description
`Enable caching and password autocomplete on login page`	Allows the user's browser to store usernames. If enabled, after an initial login, usernames are auto-filled into the `User Name` field on the login page. This preference is selected by default and caching and autocomplete are enabled.
`Enable secure and persistent browser caching to improve performance`	Enables secure data caching in the browser to improve page reload performance by avoiding additional round trips to the server. This setting is selected by default for all organizations. 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 the SMS method of identity confirmation`	Allows users to receive a one-time PIN delivered via SMS. If this option 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 organizations.
`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.
`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 organizations.
`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

Field	Description
	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 organizations.
`Enable CSRF protection on POST requests on non-setup pages`	
`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 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
- Device Activation — 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. They then have access to reports and dashboards. Alternatively, they can switch to Salesforce Classic, where they are 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**.

The 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

Identity Verification History

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

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.

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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To view network access:
- "Login Challenge Enabled"

To change network access:
- "Manage IP Addresses"

SEE ALSO:

Session Security

Restrict Where and When Users Can Log In To Salesforce

Security Implementation Guide

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. Salesforceadmins 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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

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.
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.

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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

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.
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.

Session Type	Description
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

Identity Confirmation Activations

Identity confirmation activations track information about activated devices, including login IP addresses and client browsers used.

Identity confirmation verifies the identities of users accessing Salesforce from unknown devices. It adds an extra layer of security on top of authentication. When a user comes from an unknown device, the user is challenged to verify identity using the highest-priority verification method available. In order of priority, the methods are:

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

Available in all editions

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.

   Important: Verification via push notification or location-based automated verification with the Salesforce Authenticator mobile app version 2.0 will be available following the completion of the Spring '16 Salesforce release to all production orgs on February 13, 2016. It isn't available for preview or testing in sandbox orgs beforehand. Because of App Store and Google Play release processes, it's possible that version 2.0 could be available for download before the new verification method is available in sandbox and production orgs. Users who download the new version of the app can't use version 2.0 functionality in Salesforce until the new verification method is released.

2. Verification code generated by a mobile authenticator app connected to the user's account.
3. Verification code sent via SMS to the user's verified mobile phone.
4. Verification code sent via email to the user's email address.

After the user successfully completes the identity verification challenge, the device is considered activated.

- The Activations page in Setup lists the login IP addresses and client browser information of activated devices for all users in your org. You can revoke the 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 lost device so that anyone attempting to access the org from the revoked device is challenged for identity verification. This challenge adds a needed layer of security, while making sure that users stay productive.

- Users can view their own Activations page to check their activated device's login IP addresses and client browser information. End users can only revoke the activation status for their own activated device.

  For example, a user logs in to the org. On the user's Activations page, several devices are activated, but the user has only logged in from a work laptop. The user immediately revokes the activation status of those devices 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 unknown devices can't get the texted verification code. Without the code, they fail the identity verification challenge. The user can then report the potential security breach.

IN THIS SECTION:

SEE ALSO:

Use Identity Confirmation Activations
Identity Verification History

Use Identity Confirmation Activations

View your users' identity confirmation activations and revoke activation status to prevent security breaches.

To see login IP and browser information about currently activated devices, from Setup, enter *Activations* in the Quick Find box, then select **Activations**.

You can revoke activation status by checking one or more entries in the Activated Client Browser list, clicking **Remove**, and confirming the action. Users can only view and revoke their own activated device browsers. A user who's been deactivated is challenged for identity verification at their next login attempt.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

Available in all editions

SEE ALSO:

Identity Confirmation 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.

IN THIS SECTION:

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 they can log in and access Salesforce from. 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.

Set Up Two-Factor Authentication

Admins enable two-factor authentication through permissions or profile settings. Users add the mobile authenticator app through their own personal settings.

Custom Login Flows

Login flows allow administrators to build post-authentication processes to match their business practices, associate the flow with a user profile, and send the user through that flow when logging in. Use login flows to collect registration information from users, provide a terms of service acceptance form, prompt the user for a second factor of authentication, and other customization.

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) allows you to send authentication and authorization data between affiliated but unrelated Web services. This enables you to sign on to Salesforce from a client application. Federated authentication using SAML is enabled by default for your organization.
- Delegated authentication single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server, or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the permission level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by permissions, not by organization.

The primary reasons for using delegated authentication include:

- Using a stronger type of user authentication, such as integration with a secure identity provider
- Making your login page private and accessible only behind a corporate firewall
- Differentiating your organization from all other companies that use Salesforce in order to reduce phishing attacks

You must request that this feature be enabled by Salesforce. Contact Salesforce to enable delegated authentication single sign-on for your organization.

- Authentication providers let your users log in to your Salesforce organization using their login credentials from an external service provider. Salesforce supports the OpenId Connect protocol that allows users to log in from any OpenID provider such as Google, PayPal, LinkedIn and other services supporting OpenID Connect. When authentication providers are enabled, Salesforce does not 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 to access other websites. A *service provider* is a website that hosts applications. You can enable Salesforce as an identity provider and define one or more service providers. Your users can then access other applications directly from Salesforce using single sign-on. Single sign-on can be a great help to your users: instead of having to remember many passwords, they only have to remember one. Plus, the applications can be added as tabs to your Salesforce organization, which means users don't have to switch between programs.

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 they can log in and access Salesforce from. 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 549.

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 552.

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 organization.

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.

Organization-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 organization once 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 organization'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.

  Important: Verification via push notification or location-based automated verification with the Salesforce Authenticator mobile app version 2.0 will be available following the completion of the Spring '16 Salesforce release to all production orgs on February 13, 2016. It isn't available for preview or testing in sandbox orgs beforehand. Because of App Store and Google Play release processes, it's possible that version 2.0 could be available for download before the new verification method is available in sandbox and production orgs. Users who download the new version of the app can't use version 2.0 functionality in Salesforce until the new verification method is released.

- 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. Login 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 computers 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 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. Furthermore, the single sign-on 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, then 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 being 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.

Important: Verification via push notification or location-based automated verification with the Salesforce Authenticator mobile app version 2.0 will be available following the completion of the Spring '16 Salesforce release to all production orgs on February 13, 2016. It isn't available for preview or testing in sandbox orgs beforehand. Because of App Store and Google Play release processes, it's possible that version 2.0 could be available for download before the new verification method is available in sandbox and production orgs. Users who download the new version of the app can't use version 2.0 functionality in Salesforce until the new verification method is released.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

Basic Identity Confirmation

When a user logs in, Salesforce considers the user's device. If it's not recognized, Salesforce challenges the user to verify identity using the highest-priority verification method available for that user. The following is the order of priority for verification methods.

1. Verification via push notification or location-based automated verification with the Salesforce Authenticator mobile app connected to the user's account.
2. Verification code generated by a mobile authenticator app connected to the user's account. This type of code is sometimes called a "time-based one-time password." The code value changes periodically.
3. Verification code sent via SMS to the user's verified mobile device. If users don't have a verified mobile number, they're prompted to register one when they log in to Salesforce. Registering a mobile phone number verifies it and enables this method when the user is challenged in the future.
4. Verification code sent via email to the user's email address. The code expires after 24 hours.

After verification, Salesforce doesn't have to verify the user's identity again, unless the user logs in from a new device that Salesforce doesn't recognize.

Other Applications of Two-Factor Authentication

You can 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 download and install a mobile authenticator app, such as the Salesforce Authenticator app or the Google Authenticator app, on their mobile device. They connect the app to their account in Salesforce. They use the app whenever your org's policies require two-factor authentication.

The Salesforce Authenticator mobile app (version 2.0 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.

SEE ALSO:

- Restrict Where and When Users Can Log In To Salesforce
- Custom Login Flows
- Connect Salesforce Authenticator (Version 2.0 or Later) to Your Account for Identity Verification
- Connect a One-Time Password Generator App or Device for Identity Verification
- Disconnect Salesforce Authenticator (Version 2.0 or Later) from a User's Account
- Disconnect a User's One-Time Password Generator App
- Identity Verification History

Set Up Two-Factor Authentication

Admins enable two-factor authentication through permissions or profile settings. Users add the mobile authenticator app 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.


Walk Through It: Secure Logins with Two-Factor Authentication

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

- 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.

  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
  - Implementing SMS-Based Two-Factor Authentication
  - Enhancing Security with Two-Factor Authentication

IN THIS SECTION:

Set Two-Factor Authentication Login Requirements

As a Salesforce administrator, you can require your users to use a mobile authenticator app for two-factor authentication when they log in.

Set Two-Factor Authentication Login Requirements 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.

Disconnect Salesforce Authenticator (Version 2.0 or Later) from a User's Account

Only one Salesforce Authenticator (version 2.0 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, Salesforce prompts the user to connect a new authenticator app.

Disconnect a User's One-Time Password Generator App

Only one 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, Salesforce prompts the user to connect a new authenticator app.

Set Two-Factor Authentication Login Requirements

As a Salesforce administrator, you can require your users to use a mobile authenticator app for two-factor authentication when they log in.

Set Two-Factor Authentication Login Requirements 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 2.0 or Later) to Your Account for Identity Verification

You can connect version 2.0 or later of the Salesforce Authenticator mobile app to your account. Use the app whenever Salesforce has to verify your identity. 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.

Connect a One-Time Password Generator App or Device for Identity Verification

You can connect a one-time password generator app, such as Salesforce Authenticator or Google Authenticator, to your account. Use a verification code generated by the app, sometimes called a "time-based one-time password," whenever Salesforce has to verify your identity. If your administrator requires two-factor authentication for increased security when you log in, access connected apps, or access 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. If you don't yet have the two-factor authentication requirement, you can still connect the app to your account through your personal settings.

Disconnect Salesforce Authenticator (Version 2.0 or Later) from a User's Account

Only one Salesforce Authenticator (version 2.0 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, Salesforce prompts the user to connect a new authenticator app.

Disconnect a User's One-Time Password Generator App

Only one 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, Salesforce prompts the user to connect a new authenticator app.

Set Two-Factor Authentication Login Requirements

As a Salesforce administrator, you can require your users to use a mobile authenticator app for two-factor 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.

Enhancing Security with Two-Factor Authentication

See a demonstration of Two-Factor Authentication for Salesforce, and when to use it.

Walk Through It: Secure Logins with Two-Factor Authentication

Users with the "Two-Factor Authentication for User Interface Logins" permission have to use a mobile authenticator app 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.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit profiles and permission sets:

- "Manage Profiles and Permission Sets"

SEE ALSO:

- Two-Factor Authentication
- Set Two-Factor Authentication Login Requirements for Single Sign-On, Social Sign-On, and Communities
- Connect Salesforce Authenticator (Version 2.0 or Later) to Your Account for Identity Verification
- Connect a One-Time Password Generator App or Device for Identity Verification
- Disconnect Salesforce Authenticator (Version 2.0 or Later) from a User's Account
- Disconnect a User's One-Time Password Generator App
- Custom Login Flows
- Identity Verification History

Set Two-Factor Authentication Login Requirements 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.

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.

Community members with the `High Assurance` profile requirement are prompted to connect an authenticator app during login.

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"

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 Device Activation to the High Assurance column. With this setting, users who verify their identity from an unrecognized device establish a high-assurance session. Then profile users who activate a device 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.

SEE ALSO:

- Two-Factor Authentication
- Custom Login Flows
- Connect Salesforce Authenticator (Version 2.0 or Later) to Your Account for Identity Verification
- Connect a One-Time Password Generator App or Device for Identity Verification
- Disconnect Salesforce Authenticator (Version 2.0 or Later) from a User's Account
- Disconnect a User's One-Time Password Generator App

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
- Connect a One-Time Password Generator App or Device for Identity Verification
- Set Two-Factor Authentication Login Requirements
- Identity Verification History

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

Available in: **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"

Disconnect Salesforce Authenticator (Version 2.0 or Later) from a User's Account

Only one Salesforce Authenticator (version 2.0 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, Salesforce prompts the user to connect a new authenticator app.

Important: Verification via push notification or location-based automated verification with the Salesforce Authenticator mobile app version 2.0 will be available following the completion of the Spring '16 Salesforce release to all production orgs on February 13, 2016. It isn't available for preview or testing in sandbox orgs beforehand. Because of App Store and Google Play

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

Available in all editions

release processes, it's possible that version 2.0 could be available for download before the new verification method is available in sandbox and production orgs. Users who download the new version of the app can't use version 2.0 functionality in Salesforce until the new verification method is released.

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.
4. Click **Disconnect** next to the App Registration: One-Time Password Generator field.

Note: If you don't click **Disconnect** for this field, the inaccessible app still generates valid verification codes for the account.

Users can disconnect the app from their own account on the Advanced User Details page. In personal settings, the user clicks **Disconnect** next to both the App Registration: Salesforce Authenticator and App Registration: One-Time Password Generator fields.

Disconnect a User's One-Time Password Generator App

Only one 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, 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.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

SEE ALSO:

View and Manage Users

Custom Login Flows

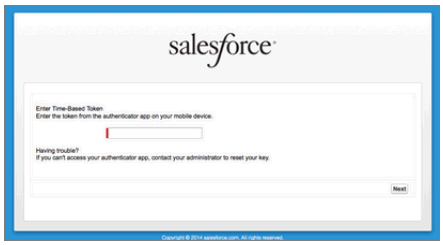
Login flows allow administrators to build post-authentication processes to match their business practices, associate the flow with a user profile, and send the user through that flow when logging in. Use login flows to collect registration information from users, provide a terms of service acceptance form, prompt the user for a second factor of authentication, and other customization.

Use the Flow Designer to create login flows, and then associate those flows with specific profiles in your organization. You can connect the same flow to multiple profiles. Users with the profile are directed to the login flow after they authenticate, but before the user is directed to the organization's content. 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



Login flows support all the 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. You can apply login flows to Salesforce organizations, communities, and portals.

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 process, then associate the finished flow with a profile.

When a user's profile is associated with a login flow, the user is directed to the flow as part of the authentication process. The login flow screens are embedded in the standard Salesforce login page. During the authentication process, these users have restricted access to the login flow screens. At the end of a successful authentication and completion of the login flow, the user is redirected to the organization. Otherwise, an explicit action can be defined within the flow to deny access.

For example, an administrator can create a login flow that implements a custom two-factor authentication process to add a desired security layer. A flow like this uses Apex methods to get the session context, extract the user's IP address, and verify if the request is coming from a Trusted IP Range. (To find or set the Trusted IP Range, from Setup, enter *Network Access* in the Quick Find box, then select **Network Access**.) If the request is coming from within a Trusted IP Range address, Salesforce skips the flow and logs the user into the organization. Otherwise, Salesforce invokes the flow providing one of three options.

1. Direct the user to log in with additional credentials, such as a time-based one-time password (TOTP).
2. Force the user to log out.
3. Direct the user to a page with more options.

You can also build login flows that direct users to customized pages, such as forms to gather more information, or pages providing users with additional information.

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 new flow using the Flow Designer and Apex.

   For example, you can design a custom IP-based two-factor authentication flow that requires a second factor of authentication only if the user is logging in from outside of the corporate Trusted IP Range. (To find or set the Trusted IP Range, from Setup, enter `Network Access` in the `Quick Find` box, then select **Network Access**.)

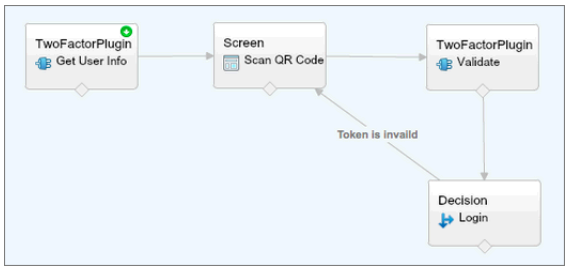
   Note: Do not set the Login IP Ranges directly in the user profile. The Login IP Ranges set directly in a profile restrict access to the organization for users of that profile who are outside that range, entirely, and those users cannot enter the login flow process.

   The flow should contain the following.

   a. A new Apex class defining an Apex plugin that implements from the (`Process.Plugin`) and uses the `Auth.SessionManagement` class to access the time-based one-time password (TOTP) methods and services. The new Apex class for the plugin 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 when the token is invalid.



Within the flow, you can set input variables. If you use the following specified names, these values will be populated for the flow when it starts.

Name	Value Description
`LoginFlow_LoginType`	The user type, such as Chatter Community external user
`LoginFlow_IpAddress`	The user's current IP address
`LoginFlow_LoginIpAddress`	The user's IP address used during login, which can change after authentication
`LoginFlow_UserAgent`	The user agent string provided by the user's browser
`LoginFlow_Platform`	The operating system for the user
`LoginFlow_Application`	Application used to request authentication
`LoginFlow_Community`	Current Community, if this login flow applies to a Community
`LoginFlow_SessionLevel`	The current session security level, Standard or High Assurance
`LoginFlow_UserId`	The user's 18-character ID.

During the flow, you can assign the following, pre-defined variables values for specific behavior.

Note: The flow loads these values only *after* a UI screen is refreshed (a user clicking a button does not load the values, a new screen must be added to the flow for the values to be loaded).

Name	Value Description
`LoginFlow_FinishLocation`	A Text value. Provide a string that defines where the user goes after completing the login flow. The string should be a valid Salesforce URL (the user cannot leave the organization and stay in the flow) or relative path.
`LoginFlow_ForceLogout`	A Boolean value. Set this variable to `true` to log the user out, immediately, and force the user to exit the flow.

2. Save the flow.
3. Activate the flow.
4. Connect the login flow to a profile.

SEE ALSO:

Custom Login Flows

Login Flow Samples

Connect a Login Flow to a Profile

Connect a Login Flow to a Profile

After you create a login flow in Flow Designer and activate the flow, you associate it with a profile in your organization. Users with that profile are then directed to the 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. Enter a name to reference the login flow association when you edit or delete it. The name doesn't need to be unique.
4. Select the login flow for the profile. The drop-down list includes all the available flows saved in the Flow Designer. Only active flows of type Flow are supported.
5. Select a user license for the profile to which you want to connect the flow. The profile list then shows profiles with that license.
6. Select the profile to connect to the login flow.
7. Click **Save**.

   Users of the profile are now directed to the login flow.

After you associate the login flow, you can edit or delete the flows listed on this login flows page.

You can associate a login flow with one or more profiles. However, a profile can't be connected to more than one login flow.

SEE ALSO:

Custom Login Flows

Create a Login Flow

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 they can log in and access Salesforce from. 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 connection type, timeout settings, and more.

Create a Login Flow

Use the Cloud Flow Designer to build a login flow process, then associate the finished flow with a profile.

Connect a Login Flow to a Profile

After you create a login flow in Flow Designer and activate the flow, you associate it with a profile in your organization. Users with that profile are then directed to the login flow.

Set Up Two-Factor Authentication

Admins enable two-factor authentication through permissions or profile settings. Users add the mobile authenticator app 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 they can log in and access Salesforce from. 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 549.

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 552.

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 organization.

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.

Organization-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 organization once 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 organization'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.

  Important: Verification via push notification or location-based automated verification with the Salesforce Authenticator mobile app version 2.0 will be available following the completion of the Spring '16 Salesforce release to all production orgs on February 13, 2016. It isn't available for preview or testing in sandbox orgs beforehand. Because of App Store and Google Play release processes, it's possible that version 2.0 could be available for download before the new verification method is available in sandbox and production orgs. Users who download the new version of the app can't use version 2.0 functionality in Salesforce until the new verification method is released.

- 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. Login 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 computers 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 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. Furthermore, the single sign-on 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, then 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 being 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.

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 Classic Mobile app can bypass IP ranges that are defined for profiles. Salesforce Classic Mobile 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 Classic Mobile on page 758 for that user.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To view login IP ranges:
- "View Setup and Configuration"

To edit and delete login IP ranges:
- "Manage Profiles and Permission Sets"

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.

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.

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"

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 Classic Mobile app can bypass IP ranges that are defined for profiles. Salesforce Classic Mobile 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 Classic Mobile on page 758 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: **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** 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**.

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.

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"

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

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.

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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To view network access:
- "Login Challenge Enabled"

To change network access:
- "Manage IP Addresses"

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.

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,

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 set password policies:
- "Manage Password Policies"

Field	Description
	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`.
`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 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 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.

Field	Description
`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. **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 organization uses the Microsoft Input Method Editor (IME) with the input mode set to Hiragana, when you type ASCII characters they're converted into Japanese characters in normal text fields. However, the IME does not work properly in fields with obscured text. If your organization'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.

Field	Description
`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: • 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:
- "Manage Internal 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 connection type, timeout settings, 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 12 hours even though you can only set it as low as 15 minutes. Select a value between 15 minutes and 12 hours. Choose a shorter timeout period if your organization 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 organization, the user must log in again.

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: **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: Do *not* select `Disable session timeout warning popup` when enabling this option.
`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. Note: This option 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 to help prevent unauthorized use of the session ID in another domain. This preference is enabled by default for organizations created with the Spring '15 release or later.
`Require secure connections (HTTPS)`	Determines whether HTTPS is required to log in to or access Salesforce, apart from Force.com sites, which can still be accessed using HTTP. This option is enabled by default for security reasons. Note: The Reset Passwords for Your Users page can only be accessed using HTTPS.
`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 option 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 option 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 is not available.
`Use POST requests for cross-domain sessions`	Sets the organization 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"/>` sometimes doesn't display.

Field	Description
`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 option is enabled, login IP ranges are enforced on each page request, including requests from client applications. If this option is not enabled, login IP ranges are enforced only when a user logs in. This option affects all user profiles that have login IP restrictions.
`Enable caching and password autocomplete on login page`	Allows the user's browser to store usernames. If enabled, after an initial login, usernames are auto-filled into the `User Name` field on the login page. This preference is selected by default and caching and autocomplete are enabled.
`Enable secure and persistent browser caching to improve performance`	Enables secure data caching in the browser to improve page reload performance by avoiding additional round trips to the server. This setting is selected by default for all organizations. 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 the SMS method of identity confirmation`	Allows users to receive a one-time PIN delivered via SMS. If this option 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 organizations.
`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.
`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 organizations.
`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.

Field	Description
`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 organizations.
`Enable CSRF protection on POST requests on non-setup pages`	
`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 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
- Device Activation — 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. They then have access to reports and dashboards. Alternatively, they can switch to Salesforce Classic, where they are 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**.

The 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

Identity Verification History

Create a Login Flow

Use the Cloud Flow Designer to build a login flow process, then associate the finished flow with a profile.

When a user's profile is associated with a login flow, the user is directed to the flow as part of the authentication process. The login flow screens are embedded in the standard Salesforce login page. During the authentication process, these users have restricted access to the login flow screens. At the end of a successful authentication and completion of the login flow, the user is redirected to the organization. Otherwise, an explicit action can be defined within the flow to deny access.

For example, an administrator can create a login flow that implements a custom two-factor authentication process to add a desired security layer. A flow like this uses Apex methods to get the session context, extract the user's IP address, and verify if the request is coming from a Trusted IP Range. (To find or set the Trusted IP Range, from Setup, enter `Network Access` in the `Quick Find` box, then select **Network Access**.) If the request is coming from within a Trusted IP Range address, Salesforce skips the flow and logs the user into the organization. Otherwise, Salesforce invokes the flow providing one of three options.

1. Direct the user to log in with additional credentials, such as a time-based one-time password (TOTP).
2. Force the user to log out.
3. Direct the user to a page with more options.

You can also build login flows that direct users to customized pages, such as forms to gather more information, or pages providing users with additional information.

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 new flow using the Flow Designer and Apex.

   For example, you can design a custom IP-based two-factor authentication flow that requires a second factor of authentication only if the user is logging in from outside of the corporate Trusted IP Range. (To find or set the Trusted IP Range, from Setup, enter `Network Access` in the `Quick Find` box, then select **Network Access**.)

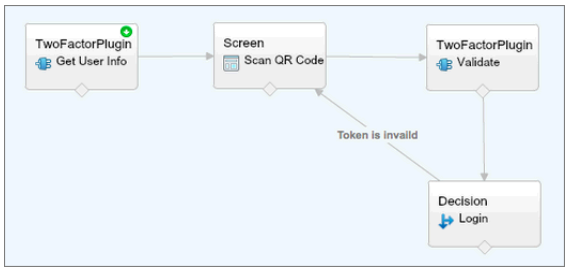
   Note: Do not set the Login IP Ranges directly in the user profile. The Login IP Ranges set directly in a profile restrict access to the organization for users of that profile who are outside that range, entirely, and those users cannot enter the login flow process.

   The flow should contain the following.

   a. A new Apex class defining an Apex plugin that implements from the (`Process.Plugin`) and uses the `Auth.SessionManagement` class to access the time-based one-time password (TOTP) methods and services. The new Apex class for the plugin 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 when the token is invalid.



Within the flow, you can set input variables. If you use the following specified names, these values will be populated for the flow when it starts.

Name	Value Description
`LoginFlow_LoginType`	The user type, such as Chatter Community external user
`LoginFlow_IpAddress`	The user's current IP address
`LoginFlow_LoginIpAddress`	The user's IP address used during login, which can change after authentication
`LoginFlow_UserAgent`	The user agent string provided by the user's browser
`LoginFlow_Platform`	The operating system for the user
`LoginFlow_Application`	Application used to request authentication
`LoginFlow_Community`	Current Community, if this login flow applies to a Community
`LoginFlow_SessionLevel`	The current session security level, Standard or High Assurance
`LoginFlow_UserId`	The user's 18-character ID.

During the flow, you can assign the following, pre-defined variables values for specific behavior.

Note: The flow loads these values only *after* a UI screen is refreshed (a user clicking a button does not load the values, a new screen must be added to the flow for the values to be loaded).

Name	Value Description
`LoginFlow_FinishLocation`	A Text value. Provide a string that defines where the user goes after completing the login flow. The string should be a valid Salesforce URL (the user cannot leave the organization and stay in the flow) or relative path.
`LoginFlow_ForceLogout`	A Boolean value. Set this variable to `true` to log the user out, immediately, and force the user to exit the flow.

2. Save the flow.
3. Activate the flow.

4. Connect the login flow to a profile.

SEE ALSO:

Custom Login Flows

Login Flow Samples

Connect a Login Flow to a Profile

Connect a Login Flow to a Profile

After you create a login flow in Flow Designer and activate the flow, you associate it with a profile in your organization. Users with that profile are then directed to the 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. Enter a name to reference the login flow association when you edit or delete it. The name doesn't need to be unique.
4. Select the login flow for the profile. The drop-down list includes all the available flows saved in the Flow Designer. Only active flows of type Flow are supported.
5. Select a user license for the profile to which you want to connect the flow. The profile list then shows profiles with that license.
6. Select the profile to connect to the login flow.
7. Click **Save**.

   Users of the profile are now directed to the login flow.

After you associate the login flow, you can edit or delete the flows listed on this login flows page.

You can associate a login flow with one or more profiles. However, a profile can't be connected to more than one login flow.

SEE ALSO:

Custom Login Flows

Create a Login Flow

Set Up Two-Factor Authentication

Admins enable two-factor authentication through permissions or profile settings. Users add the mobile authenticator app through their own personal settings.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

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.

  Walk Through It: Secure Logins with Two-Factor Authentication
- 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.

  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
  - Implementing SMS-Based Two-Factor Authentication
  - Enhancing Security with Two-Factor Authentication

IN THIS SECTION:

Set Two-Factor Authentication Login Requirements

As a Salesforce administrator, you can require your users to use a mobile authenticator app for two-factor authentication when they log in.

Set Two-Factor Authentication Login Requirements 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.

Disconnect Salesforce Authenticator (Version 2.0 or Later) from a User's Account

Only one Salesforce Authenticator (version 2.0 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, Salesforce prompts the user to connect a new authenticator app.

Disconnect a User's One-Time Password Generator App

Only one 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, Salesforce prompts the user to connect a new authenticator app.

Set Two-Factor Authentication Login Requirements

As a Salesforce administrator, you can require your users to use a mobile authenticator app for two-factor authentication when they log in.

Set Two-Factor Authentication Login Requirements 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 2.0 or Later) to Your Account for Identity Verification

You can connect version 2.0 or later of the Salesforce Authenticator mobile app to your account. Use the app whenever Salesforce has to verify your identity. 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.

Connect a One-Time Password Generator App or Device for Identity Verification

You can connect a one-time password generator app, such as Salesforce Authenticator or Google Authenticator, to your account. Use a verification code generated by the app, sometimes called a "time-based one-time password," whenever Salesforce has to verify your identity. If your administrator requires two-factor authentication for increased security when you log in, access connected apps, or access 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. If you don't yet have the two-factor authentication requirement, you can still connect the app to your account through your personal settings.

Disconnect Salesforce Authenticator (Version 2.0 or Later) from a User's Account

Only one Salesforce Authenticator (version 2.0 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, Salesforce prompts the user to connect a new authenticator app.

Disconnect a User's One-Time Password Generator App

Only one 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, Salesforce prompts the user to connect a new authenticator app.

Set Two-Factor Authentication Login Requirements

As a Salesforce administrator, you can require your users to use a mobile authenticator app for two-factor 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.

Enhancing Security with Two-Factor Authentication

See a demonstration of Two-Factor Authentication for Salesforce, and when to use it.

Walk Through It: Secure Logins with Two-Factor Authentication

Users with the "Two-Factor Authentication for User Interface Logins" permission have to use a mobile authenticator app 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

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To edit profiles and permission sets:

- "Manage Profiles and Permission Sets"

- 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 for Single Sign-On, Social Sign-On, and Communities
- Connect Salesforce Authenticator (Version 2.0 or Later) to Your Account for Identity Verification
- Connect a One-Time Password Generator App or Device for Identity Verification
- Disconnect Salesforce Authenticator (Version 2.0 or Later) from a User's Account
- Disconnect a User's One-Time Password Generator App
- Custom Login Flows
- Identity Verification History

Set Two-Factor Authentication Login Requirements 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.

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.

Community members with the `High Assurance` profile requirement are prompted to connect an authenticator app during login.

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"

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 Device Activation to the High Assurance column. With this setting, users who verify their identity from an unrecognized device establish a high-assurance session. Then profile users who activate a device 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.

SEE ALSO:

Two-Factor Authentication
Custom Login Flows
Connect Salesforce Authenticator (Version 2.0 or Later) to Your Account for Identity Verification
Connect a One-Time Password Generator App or Device for Identity Verification
Disconnect Salesforce Authenticator (Version 2.0 or Later) from a User's Account
Disconnect a User's One-Time Password Generator App

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
- Connect a One-Time Password Generator App or Device for Identity Verification
- Set Two-Factor Authentication Login Requirements
- Identity Verification History

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

Available in: **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 2.0 or Later) to Your Account for Identity Verification

You can connect version 2.0 or later of the Salesforce Authenticator mobile app to your account. Use the app whenever Salesforce has to verify your identity. 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.

Important: Verification via push notification or location-based automated verification with the Salesforce Authenticator mobile app version 2.0 will be available following the completion of the Spring '16 Salesforce release to all production orgs on February 13, 2016. It isn't available for preview or testing in sandbox orgs beforehand. Because of App Store and Google Play release processes, it's possible that version 2.0 could be available for download before the new verification method is available in sandbox and production orgs. Users who download the new version of the app can't use version 2.0 functionality in Salesforce until the new verification method is released.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

The Salesforce Authenticator (version 2.0 or later) app on your mobile device is the second "factor" of authentication. Using the app adds an extra level of security to your account. Once connected, the app sends a notification to your mobile device whenever you perform an activity that requires identity verification. When you get the notification, you open the app on your mobile device, check the activity details, and respond on your mobile device to verify. If you get a notification 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 you can use as an alternate method of identity verification.

1. Download and install version 2.0 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 2.0 through the App Store or Google Play. The update preserves any connected accounts you already have in the app. These are "code-only" accounts that generate verification codes but do not send push notifications or allow location-based automated verifications. You can recognize a code-only account on your Connected Accounts list in the app by the verification code that appears below the account name. 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 2.0 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. Enter the phrase in the `Two-Word Phrase` field in Salesforce.
8. Click **Connect**.

   If you previously connected an authenticator app that generates verification codes to your account, you sometimes see an alert. Connecting version 2.0 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. Tap **Connect** in the app to complete the account connection.

Connect a One-Time Password Generator App or Device for Identity Verification

You can connect a one-time password generator app, such as Salesforce Authenticator or Google Authenticator, to your account. Use a verification code generated by the app, sometimes called a "time-based one-time password," whenever Salesforce has to verify your identity. If your administrator requires two-factor authentication for increased security when you log in, access connected apps, or access 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. If you don't yet have the two-factor authentication requirement, you can still connect the app to your account through your personal settings.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

Available in all editions

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**.

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, you can 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**.

Disconnect Salesforce Authenticator (Version 2.0 or Later) from a User's Account

Only one Salesforce Authenticator (version 2.0 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, Salesforce prompts the user to connect a new authenticator app.

Important: Verification via push notification or location-based automated verification with the Salesforce Authenticator mobile app version 2.0 will be available following the completion of the Spring '16 Salesforce release to all production orgs on February 13, 2016. It isn't available for preview or testing in sandbox orgs beforehand. Because of App Store and Google Play release processes, it's possible that version 2.0 could be available for download before the new verification method is available in sandbox and production orgs. Users who download the new version of the app can't use version 2.0 functionality in Salesforce until the new verification method is released.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

Available in all editions

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.
4. Click **Disconnect** next to the `App Registration: One-Time Password Generator` field.

   Note: If you don't click **Disconnect** for this field, the inaccessible app still generates valid verification codes for the account.

Users can disconnect the app from their own account on the Advanced User Details page. In personal settings, the user clicks **Disconnect** next to both the `App Registration: Salesforce Authenticator` and `App Registration: One-Time Password Generator` fields.

Disconnect a User's One-Time Password Generator App

Only one 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, Salesforce prompts the user to connect a new authenticator app.

EDITIONS

Available in: Both Salesforce Classic and Lightning Experience

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

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

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: both Salesforce Classic and 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 you specify. For each policy, you define real-time actions, such as notify, block, force two-factor authentication, or choose a session to end.

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.

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 you specify. For each policy, you define real-time actions, such as notify, block, force two-factor authentication, or choose a session to end.

When you enable Transaction Security for your org, two policies are created:

- Concurrent Sessions Limiting policy to limit concurrent login sessions
- Data Loader Lead Export policy to block excessive data downloads done through APIs

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 Sessions Limiting 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.

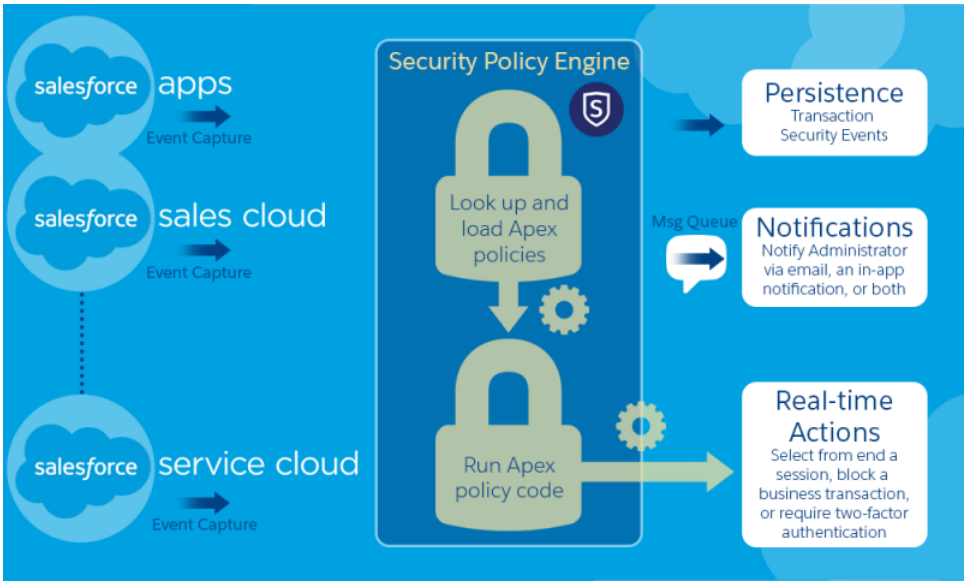
EDITIONS

Available in: both Salesforce Classic and 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.



A transaction security policy consists of events, notifications, and actions.

- Policies to apply to the organization, made up of events. Available event types are:
  - Data Export for Account, Contact, Lead, and Opportunity objects
  - Entity for authentication providers and sessions, client browsers, and login IP
  - Logins
  - Resource Access for connected apps and reports and dashboards
- Available policy notifications—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

- End a current session

You can also take no action and only receive a notification. The actions available depend on the event type selected.

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: both Salesforce Classic and Lightning Experience

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

Requires purchasing Salesforce Shield or Salesforce Shield Event Monitoring add-on subscriptions.

USER PERMISSIONS

To create, edit, and manage transaction security policies:

- "Author Apex"

  AND

  "Customize Application"

1. Enable transaction security policies to make them available for use. This task is done once when you first go to Transaction Security.
   a. From Setup, enter *Transaction Security* in the Quick Find box, then select **Transaction Security**.
   b. To enable the policy list view and install the supplied policies, 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 Data Loader Lead Export policy blocks excessive data downloads done through APIs. It's triggered when someone uses an API call that runs for more than one second to download more than 2,000 lead records. 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.

   Selecting **When users exceed the maximum number of Salesforce sessions allowed, close the oldest session.** prevents this problem. When a programmatic request is made that requires a login but no more sessions are allowed, older sessions are ended until the number of sessions 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.
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 Authenticating 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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Requires purchasing Salesforce Shield or Salesforce Shield Event Monitoring add-on subscriptions.

USER PERMISSIONS

To create, edit, and manage transaction security policies:
- "Author Apex"

  AND

  "Customize Application"

1. From Setup, enter *Transaction Security* in the Quick Find box, select **Transaction Security**, and then click **New** in Custom 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 organization. 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.
     - **Data Export**—Notifies you if the selected object type has been exported using the Data Loader API client.
     - **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. Email and In-App notifications are always available. For login and resource events, you can also block the action or require a higher level of access control with two-factor authentication. For login events, you can require ending an existing session before continuing with 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 Salesforce1 or Lightning Experience for the AccessResource event type. The Block action is used instead.

     Important: Don't create a policy requiring the two-factor authentication action without first providing 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.
   - 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.

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.

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.

Your `TxnSecurity.PolicyCondition` implementation isn't deleted when you delete a transaction security policy. 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: both Salesforce Classic and 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

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: both Salesforce Classic and Lightning Experience

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

Requires purchasing Salesforce Shield or Salesforce Shield Event Monitoring add-on subscriptions.

USER PERMISSIONS

To create, edit, and manage transaction security policies:

- "Author Apex"

  AND

  "Customize Application"

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: both Salesforce Classic and 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 Salesforce1 user. The notification lists the policy that was triggered. Here's an example.

Example:

```
Transaction Security Alert:
Policy New Encrypted Custom Field was triggered.
```

My Domain

Enhance access security and brand your organization's pages by enabling your custom domain.

Using My Domain, you can define a custom Salesforce domain name. A custom domain name helps you better manage login and authentication for your organization in several key ways.

- 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.
- Access increased support for single sign-on. My Domain is required to use some Salesforce Identity features, such as authentication providers and identity providers.
- Set custom login policy and determine how users are authenticated.
- Let users select an alternate identity provider from the login page.

Watch a Demo (5:11 minutes)

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

You can define a custom domain name only one time. My Domain is also available for sandbox environments.

Note: My Domain is subject to additional Terms of Use.

Your domain name uses standard URL format, including:

- The protocol: https://
- The subdomain prefix: your brand or term
- The domain: my.salesforce.com

For example, a company called Universal Containers wants to use the subdomain `universalcontainers`. The company's login URL would be `https://universalcontainers.my.salesforce.com/`. You can use up to 40 characters.

Salesforce is automatically 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 organization by customizing your domain's login policy.

You must enable My Domain if you want to use Lightning components in Lightning component tabs, Lightning Pages, the Lightning App Builder, or standalone apps.

Important: After you deploy your new domain name, you can't reverse it.

IN THIS SECTION:

Set Up a Domain Name

Implementing your custom domain name is quick and easy.

Define Your Domain Name

Sign up for your organization's custom domain name.

Guidelines and Best Practices for Implementing My Domain

These tips help smooth the transition to a new domain name.

Test and Deploy Your New Domain Name

After you set up your domain name, test it and then roll it out to your users.

My Domain URL Changes

Set the My Domain Login Policy

Secure your login by customizing the login policy for your domain.

Customize Your Login Page Branding

Customize the look and feel of your login page by adding a background color, logo, and right-side iFrame content. Customizing your login page helps users recognize your page by tying it to your company's branding.

Add Identity Providers on a Login Page

Allow users to authenticate using alternate identity provider options right from your login page.

Get System Performance and Maintenance Information Using My Domain

Salesforce customers get system performance and maintenance information from `trust.salesforce.com`.

My Domain FAQ

SEE ALSO:

Set Up a Domain Name

My Domain URL Changes

Test and Deploy Your New Domain Name

Guidelines and Best Practices for Implementing My Domain

Get System Performance and Maintenance Information Using My Domain

Set Up a Domain Name

Implementing your custom domain name 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 organization.
5. Set the login policy for users accessing your pages.

SEE ALSO:

- My Domain
- Define Your Domain Name
- Test and Deploy Your New Domain Name
- Set the My Domain Login Policy
- Customize Your Login Page Branding
- Add Identity Providers on a Login Page

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To set up a domain name:
- "Customize Application"

Define Your Domain Name

Sign up for your organization's custom domain name.

Start setting up your custom domain name by finding a domain name unique to your organization and signing up for it.

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, a company called Universal Containers wants to use the subdomain `universalcontainers`. The company's login URL would be `https://universalcontainers.my.salesforce.com/`. You can use up to 40 characters.

   You can't use these reserved words for subdomains:

   - www
   - salesforce
   - heroku

   And, you can't start the domain name with:

   - root
   - status
3. Click **Check Availability**. If your name is already taken, choose a different one.
4. Click **Terms and Conditions** to review your agreement, then select the checkbox.
5. Click **Register Domain**.
6. You receive an email when your domain name is ready for testing. (It can take from 30 seconds to 24 hours.)

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To define a domain name:
- "Customize Application"

Your domain isn't rolled out until you've tested and deployed it.

SEE ALSO:

- Set Up a Domain Name
- Guidelines and Best Practices for Implementing My Domain
- My Domain URL Changes
- Test and Deploy Your New Domain Name

Guidelines and Best Practices for Implementing My Domain

These tips help smooth the transition to a new domain name.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

- Test in a sandbox first, because you can't set login policies before deploying your domain. To test these customizations, custom UI features, Visualforce pages, and application URL changes, define and deploy a domain name in a sandbox environment.
- Deploy your new domain when your organization 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 custom elements thoroughly before deploying your domain name. Your customizations should not use instance-based URLs.
- Make sure that you update any application URLS that were created before you enabled 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 will show My Domain URLs 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, will still contain the old URLs. After your domain is deployed, those links will show the new My Domain URLs.
- Help your users get started using your new domain name by providing links to pages they use frequently, such as your login page. Let your users know if the login policy will be changed and encourage them to update their bookmarks the first time they're redirected.
- Only use `Prevent login from https://login.salesforce.com` if you're concerned that users who are not aware of your custom domain might try to use it. Otherwise, leave the option available to your users as they get used to the new domain name.
- 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 domain name.

  You can use your domain's login policy settings to gradually phase in your domain name for your users. Redirecting users with a warning for a few days or weeks before requiring users to use the new domain name to access your pages gives them time to change their bookmarks.

- Bookmarks do not 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 *`na1.salesforce.com`* with *`<mydomain>.my.salesforce.com`* in the bookmark's URL.
- If you block application page requests that don't use the new Salesforce domain name URLs, let your users know they need to either update old bookmarks or create new ones for the login page as well as any tabs or links within the application. Users will be required to use the new URLs immediately if you change your login redirect policy to `Not Redirected`.
- 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.

- Communicate the upcoming change to your users before deploying it.
- On the `login.salesforce.com` page, users can click the **Log in to a custom domain** link to provide your custom domain name and log in. In this case, they need to know the domain name. However, you should give them a direct link to your custom domain's login page.

If you have the following.	You should do the following.
API integrations into your organization	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 custom domain is deployed, Salesforce returns the server URL containing your domain. Even though the redirect policy settings have no effect on API calls (the old calls to instance URLs should continue to work) the best practice is to use the value returned by Salesforce.
Email templates	Replace references to the organization's instance URL with your custom domain.
Custom Visualforce pages or custom Force.com apps	Replace references to the organization's instance URL with your custom domain. 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. Save the page, and the system populates the field with your new My Domain URL.

SEE ALSO:

My Domain URL Changes

Test and Deploy Your New Domain Name

My Domain

Test and Deploy Your New Domain Name

After you set up your domain name, test it and then roll it out to your users.

Before deploying your domain to your users, you can log in to test your domain. Testing gives you the chance to explore your domain name and helps you verify addresses for important pages that your users will need to use after your domain rolls out.

Important: After you deploy your new domain name, you can't reverse it.

1. Test your domain login. From Setup, enter *My Domain* in the `Quick Find` box, then select **My Domain**, then click **Click here to login**. Or, click the URL in the email to log in to Salesforce using your new domain name.

   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 domains in sandbox environments. However, before deploying your domain, you can't set a login policy, such as preventing users from logging in at login.salesforce.com.

2. Test the new domain name by clicking tabs and links. All pages 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 custom elements thoroughly before deploying your domain name. Your customizations should not use instance-based URLs.

3. To roll out the new domain name to your organization, from Setup, enter *My Domain* in the `Quick Find` box, then select **My Domain** and then click **Deploy to Users**.

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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To set up a domain name:
- "Customize Application"

SEE ALSO:

- Set Up a Domain Name
- Guidelines and Best Practices for Implementing My Domain
- Customize Your Login Page Branding
- Add Identity Providers on a Login Page
- Set the My Domain Login Policy

My Domain URL Changes

When you set up a domain name for your organization, all of your application URLs, including those of Visualforce pages, will change. Make sure that you update any application URLS that were created before you enabled 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://na1.salesforce.com/<pageID>`	`https://<subdomain>.my.salesforce.com/<pageID>`

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

URL Type	Old URL	New URL
Visualforce page with no namespace	`https://c.na1.visual.force.com/apex/<pagename>`	`https://<subdomain>--c.na1.visual.force.com/apex/<pagename>`
Visualforce page *with* namespace	`https://<yournamespace101>.na1.visual.force.com/apex/<pagename>`	`https://<subdomain>--<yournamespace>.na1.visual.force.com/apex/<pagename>`

Note: If you implement My Domain in a sandbox environment, the URL format is `https://<subdomain>--<sandboxname>.<instance>.my.salesforce.com`. Since you can't have namespaces in a sandbox environment, the format of all Visualforce page URLs in a sandbox is `https://<subdomain>--<sandboxname>.<instance>.my.salesforce.com/apex/<pagename>`.

SEE ALSO:

My Domain

Guidelines and Best Practices for Implementing My Domain

Set the My Domain Login Policy

Secure your login by customizing the login policy for your domain.

Customize your login policy to add a layer of security for your organization. By default, users may log in from a generic Salesforce login page, bypassing the login page specific to your domain. Users are also allowed to 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 turn off authentication for users who do not use your domain-specific login page, select the login policy. For example, this will prevent users from logging in at the generic `https://<instance>.salesforce.com/` login page, and being redirected to your pages after login. This option enhances security by preventing login attempts by anyone who does not know your domain name.
4. Choose a redirect policy.
   a. Choose `Redirect to the same page within the domain` to allow users to continue using URLs that do not include your domain name. Choosing this option does not enhance security for your organization.

      Note: Bookmarks do not 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 *na1.salesforce.com* with *<mydomain>.my.salesforce.com* in the bookmark's URL.

   b. Choose `Redirected with a warning to the same page within the domain` to warn users that they should be using your domain name. After reading the warning, users will be allowed to view the page. Selecting this option for a few days or weeks can help users transition to a new domain name, but does not enhance security for your organization.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To set login policy for a domain:

- "Customize Application"

c. Choose `Not redirected` to require users to use your domain name when viewing your pages. This option provides the greatest level of security.

5. Click **Save**.

SEE ALSO:

Set Up a Domain Name

Guidelines and Best Practices for Implementing My Domain

Customize Your Login Page Branding

Customize the look and feel of your login page by adding a background color, logo, and right-side iFrame content. Customizing your login page helps users recognize your page by tying it to your company's branding.

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. 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 is designed to resize to fill approximately 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, you can use the My Domain Sample template.

   Example: https://c.salesforce.com/login-messages/promos.html
6. 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 accounts from those services. Configure authentication services as Auth. Providers in Setup.
7. Click **Save**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To customize a login page:

- "Customize Application"

SEE ALSO:

Set Up a Domain Name

Add Identity Providers on a Login Page

Set the My Domain Login Policy

About External Authentication Providers

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 alternate identity providers on your domain's login page. Users are sent to the alternate identity provider's login screen to authenticate and then are 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. Janrain can't be used 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 Domain Name
- Customize Your Login Page Branding
- Set the My Domain Login Policy
- About External Authentication Providers

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To add identity providers on a login page:

- "Customize Application"

Get System Performance and Maintenance Information Using My Domain

Salesforce customers get system performance and maintenance information from `trust.salesforce.com`.

Here's how to get that information using your new domain name.

1. Go to trust.salesforce.com where you can check the System Status.
2. To find the instance for your domain, click **What instance am I using?**
3. In the System Status table, look for the entry for your instance.

SEE ALSO:

- My Domain

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To set up a domain name:

- "Customize Application"

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, administrators can define a custom Salesforce domain name for their organization. The custom domain name appears in all organization URLs and replaces the instance name (such as `na1`). URLs for organizations using My Domain use the format `https://<mydomain>.my.salesforce.com` (such as `https://mydomain.my.salesforce.com`).

My Domain is not used as a 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 My Domain's advantages?

My Domain allows customers to:

- Customize the login page with their own branding.
- Use Identity features for single sign-on. My Domain is required for:
  - Single sign-on into a Salesforce organization
  - Using a Salesforce organization as an identity provider for single sign-on into third-party applications or other Salesforce organizations
- Preserve deep links (such as `https://<mydomain>.my.salesforce.com/001/o`) through any future organization splits and migrations.

Does My Domain work differently in different Salesforce Editions?

The only difference is that Developer Edition URLs are appended with "-developer-edition".

Does My Domain work in sandboxes?

Sandboxes and production organizations 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 organization is copied into sandbox.

For example, if the production organization name is `acme.my.saleforce.com`, the sandbox name is `acme--<sandboxName>.csN.my.salesforce.com`.

You should test your custom domain in a sandbox before deploying it to find any hard-coded references to URLs in Visualforce pages, email templates, or other content.

What are the differences between the Redirect Policy options?

After you deploy your domain, you can select a redirect option for users trying to access a page in your organization without using the custom domain 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 any notification.

If `Redirected with a warning to the same page within the domain` is selected, users briefly see a standard warning message before being redirected to the new URL. The warning gives users a chance to change their bookmarks and start getting used to using the new domain name. The message can't be customized.

If `Not redirected` is selected, the user sees the page is missing. This is recommended as the most secure option, but it is a best practice to use `Redirected with a warning to the same page within the domain` for a short period of time after your custom domain is deployed so users get used to the new URLs.

How does My Domain work with single sign-on?

My Domain is required for single sign-on implementation. For inbound single sign-on requests, the custom domain enables deep linking directly to pages in the organization. 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 organization deploys My Domain and has `Prevent login from https://login.salesforce.com` for users selected in the My Domain Settings.

Note: If you're using external Chatter groups along with single sign-on for employees, then users outside of your company are redirected to a SAML identity provider they can't access. For your implementation to work, migrate external Chatter groups to communities, or in the My Domain settings do *not* select `Prevent login from https://login.salesforce.com`. This allows users to continue to login through `login.salesforce.com`.

Is My Domain available for the API?

Yes, you can use the Salesforce APIs with your My Domain.

Is the subdomain for My Domain related to the subdomain for Sites?

No. The subdomains you use for Sites and My Domain can be the same or different.

Is there a limit on how long our subdomain can be?

Yes. You can use 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://na1.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 rename or remove my custom domain name?

You can't change your custom domain name, or reverse its deployment, once deployed. If you have a special need to change it, contact Salesforce Customer Support.

App Launcher

The App Launcher presents users with logos that link to their on-premise applications, connected apps, and Salesforce apps, all from a unified user interface. Administrators can set the default app order for their organizations.

All Lightning Experience users get the App Launcher.

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 they are authorized to see.

In Salesforce Classic, administrators using the System Administrator profile automatically have access to the App Launcher. Administrators using profiles cloned from the System Administrator profile don't.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

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:

Salesforce Identity Implementation Guide

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.

EDITIONS

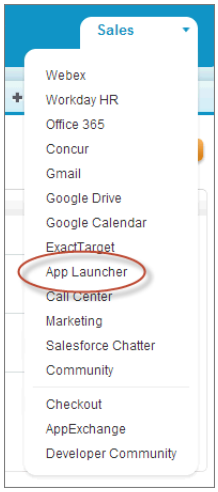
Available in: Salesforce Classic

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

Note: These steps work in Salesforce Classic. If you see a row of tabs across the top of your screen, you're in Salesforce Classic. If you see a navigation bar on the left, you're in Lightning Experience.

In Salesforce Classic, administrators using the System Administrator profile automatically have access to the App Launcher. Administrators 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

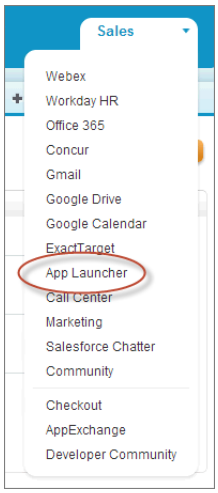
Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Note: These steps work in Salesforce Classic. If you see a row of tabs across the top of your screen, you're in Salesforce Classic. If you see a navigation bar on the left, you're in Lightning Experience.

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

For security reasons, your organization may want to configure 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 may pose a security risk, select `Don't allow HTML uploads as attachments or document records`.

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

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

   - If your organization uses the partner portal to give your partner users access to Salesforce, we don't recommend enabling this setting. Enabling this setting prevents your organization from customizing the appearance of your partner portal.
   - HTML attachments are not permitted on solutions, regardless of whether this security setting is enabled. In addition, this setting does not affect attachments on email templates; HTML attachments on email templates are always permitted.
   - After this setting is enabled, previously-uploaded HTML documents and attachments are unaffected. However, when users attempt to view an HTML attachment or

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

USER PERMISSIONS

To configure file upload and download settings:

- "Customize Application"

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**.

Single Sign-On

Single sign-on allows users to access all authorized network resources without having to log in separately to each resource. You validate usernames and passwords against your corporate user database or other client application rather than having separate user passwords managed by Salesforce.

Salesforce offers the following ways to use single sign-on:

- Federated authentication using Security Assertion Markup Language (SAML) allows you to send authentication and authorization data between affiliated but unrelated Web services. This enables you to sign on to Salesforce from a client application. Federated authentication using SAML is enabled by default for your organization.
- Delegated authentication single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server, or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the permission level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by permissions, not by organization.

  The primary reasons for using delegated authentication include:

  - Using a stronger type of user authentication, such as integration with a secure identity provider
  - Making your login page private and accessible only behind a corporate firewall
  - Differentiating your organization from all other companies that use Salesforce in order to reduce phishing attacks

  You must request that this feature be enabled by Salesforce. Contact Salesforce to enable delegated authentication single sign-on for your organization.
- Authentication providers let your users log in to your Salesforce organization using their login credentials from an external service provider. Salesforce supports the OpenId Connect protocol that allows users to log in from any OpenID provider such as Google, PayPal, LinkedIn and other services supporting OpenID Connect. When authentication providers are enabled, Salesforce does not validate a user's password. Instead, Salesforce uses the user's login credentials from the external service provider to establish authentication credentials.

When you have an external identity provider, and configure single sign-on for your Salesforce organization, Salesforce is then acting as a *service provider*. You can also enable Salesforce as an identity provider, and use single sign-on to connect to a different service provider. Only the service provider needs to configure 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"

The Single Sign-On Settings page displays which version of single sign-on is available for your organization. To learn more about the single sign-on settings, see Configuring SAML Settings for Single Sign-On. For more information about SAML and Salesforce security, see the *Security Implementation Guide*.

Benefits of Single Sign-On

Implementing single sign-on can offer the following advantages to your organization:

- **Reduced Administrative Costs:** With single sign-on, users only need to memorize a single password to access both network resources or external applications and Salesforce. When accessing Salesforce from inside the corporate network, users are logged in seamlessly, without being prompted to enter 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 administrators receive fewer requests to reset forgotten passwords.
- **Leverage Existing Investment:** Many companies use a central LDAP database to manage user identities. By delegating Salesforce authentication to this system, when a user is removed from the LDAP system, they can no longer access Salesforce. Consequently, users who leave the company automatically lose access to company data after their departure.
- **Time Savings:** On average, a user takes five to 20 seconds to log in to an online application; longer if they mistype their username or password and are prompted to reenter them. With single sign-on in place, the need to manually log in to Salesforce is avoided. These saved seconds 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 on a regular basis. For example, users can send email messages that contain links to information in Salesforce such as records and reports. When the recipients of the email message click the links, the corresponding Salesforce page opens automatically.
- **Increased Security:** Any password policies that you have established for your corporate network will also be 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:

Identity Providers and Service Providers

An *identity provider* is a trusted provider that lets you use single sign-on to access other websites. A *service provider* is a website that hosts applications. You can enable Salesforce as an identity provider and define one or more service providers. Your users can then access other applications directly from Salesforce using single sign-on. Single sign-on can be a great help to your users: instead of having to remember many passwords, they only have to remember one. Plus, the applications can be added as tabs to your Salesforce organization, which means users don't have to switch between programs.

Configuring Remote Settings

Named Credentials

A named credential specifies the URL of a callout endpoint and its required authentication parameters in one definition. You can simplify the setup of authenticated callouts by specifying a named credential as the callout endpoint. You can instead specify a URL as the callout endpoint and register that URL in your organization's remote site settings. However, in that case, you handle the authentication yourself, for example, in your code for an Apex callout. Doing so can be less secure and is especially complicated for OAuth authentication.

About Identity Connect

Identity Connect provides Active Directory integration.

Best Practices for Implementing Single Sign-On

Salesforce offers the following ways to use single sign-on:

- Federated authentication using Security Assertion Markup Language (SAML) allows you to send authentication and authorization data between affiliated but unrelated Web services. This enables you to sign on to Salesforce from a client application. Federated authentication using SAML is enabled by default for your organization.
- Delegated authentication single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server, or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the permission level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by permissions, not by organization.

  The primary reasons for using delegated authentication include:

  - Using a stronger type of user authentication, such as integration with a secure identity provider
  - Making your login page private and accessible only behind a corporate firewall
  - Differentiating your organization from all other companies that use Salesforce in order to reduce phishing attacks

  You must request that this feature be enabled by Salesforce. Contact Salesforce to enable delegated authentication single sign-on for your organization.
- Authentication providers let your users log in to your Salesforce organization using their login credentials from an external service provider. Salesforce supports the OpenId Connect protocol that allows users to log in from any OpenID provider such as Google, PayPal, LinkedIn and other services supporting OpenID Connect. When authentication providers are enabled, Salesforce does not 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 the following best practices when implementing delegated authentication single sign-on for your organization.

- Your organization's implementation of the Web service must be accessible by Salesforce servers. This means 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 cannot connect, or the request takes longer than 10 seconds to process, the login attempt fails. An error is reported to the user indicating that his or her 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 to ensure accuracy.
- For security reasons, you should make your Web service available by TLS. You must use a certificate from a trusted provider, such as Verisign or Thawte. For a full 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. Note that the Salesforce feature that validates login IP ranges continues to be in effect for single sign-on users. For more information, see Restrict Where and When Users Can Log In To Salesforce on page 529.
- You may need to map your organization's internal usernames and Salesforce usernames. If your organization does not follow a standard mapping, you may be able to extend 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 do not enable single sign-on for system administrators. If your system administrators are single sign-on users and your single sign-on server has an outage, they have no way to log in to Salesforce. System administrators should always be able to log in to Salesforce so they can disable single sign-on in the event of a problem.
- We recommend that you use a Developer Edition account or a sandbox when developing a single sign-on solution before implementing it in your organization. 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 the following best practices when implementing federated single sign-on with SAML for your organization.

- Obtain the `Salesforce Login URL` value from the Single Sign On Settings configuration page and put it in the corresponding configuration parameter of your Identity Provider (sometimes called the "Recipient URL").
- Salesforce allows a maximum of three minutes for clock skew with your IDP server; make sure your server's clock is up-to-date.
- If you are unable to log in with SAML assertion, always check the login history and note the error message. Use the SAML Assertion Validator on the Single Sign On Settings configuration page to troubleshoot.
- You need to map your organization's internal usernames and Salesforce usernames. You have two choices to do this: add a unique identifier to the `FederationIdentifier` field of each Salesforce user, or 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 User ID 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 organization preference and provide all the necessary configurations.
- Use the My Domain feature to prevent users from logging in to Salesforce directly, and gives administrators 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://<my_domain_name>.my.salesforce.com/?saml=02HKiP...`

- We recommend that you use Developer Edition account or a sandbox when testing a SAML single sign-on 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 `http://cs1.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 single sign-on configuration. The default value is `https://saml.salesforce.com`.

Single Sign-On for Portals Best Practices

Customer Portals and partner portals are not available for new organizations in the Summer '13 release or later. Use Communities instead. For more information about single sign-on and SAML for Communities, see "Configuring SAML for Communities" in Getting Started With Communities. If you continue to use portals, note the following information.

- 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 for single sign-on for portals. 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 organization.

Single Sign-On 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 for single sign-on for Sites. If only one is specified, the user receives an error.
- If all three of 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 that portal login.
- More than one portal can be used with a single organization.

SEE ALSO:

Single Sign-On

Single Sign-On Implementation Guide

Understanding Delegated Authentication Single Sign-On

Salesforce uses the following process for authenticating users using delegated authentication single sign-on:

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, then Salesforce does not validate the username and password. Instead, a Web services call is made to the user's organization, asking it to validate the username and password.

   Note: Salesforce doesn't store, log, or view the password in any way. It is disposed of immediately once the process is complete.

3. The Web services call passes the `username`, `password`, and `sourceIp` to your Web service. (`sourceIp` is the IP address that originated the login request. You must create and deploy an implementation of the Web service that can be accessed by Salesforce servers.)
4. Your implementation of the Web service validates the passed information and returns either `true` or `false`.
5. If the response is `true`, then the login process continues, a new session is generated, and the user proceeds to the application. If `false` is returned, then the user is informed that his or her username and password combination is invalid.

Note: There may be a momentary delay before a user can log in after being given delegated authentication due to the time required for the user account to become available in the organization.

SEE ALSO:

Single Sign-On

Administrator setup guide: Single Sign-On Implementation Guide

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"

Configuring Salesforce for Delegated Authentication

To enable delegated authentication single sign-on (SSO) for your organization:

1. Contact Salesforce to enable delegated authentication single sign-on for your organization.
2. Build your single sign-on Web service:
   a. In Salesforce, download the Web Services Description Language (WSDL) file `AuthenticationService.wsdl` from Setup by entering *`Download Delegated Authentication WSDL`* in the `Quick Find` box, then selecting **Download Delegated Authentication WSDL**. The WSDL describes the delegated authentication single sign-on service and can be used to automatically generate a server-side stub to which you can add your specific implementation. For example, in the WSDL2Java tool from Apache Axis, you can use the `--server-side` switch. In the wsdl.exe tool from .NET, you can use the `/server` switch.

      For a sample request and response, see Sample SOAP Message for Delegated Authentication on page 605.

   b. Add a link to your corporate intranet or other internally-accessible site that takes the authenticated user's credentials and passes them through an HTTP POST to the Salesforce login page.

      Because Salesforce does not use the `password` field other than to pass it back to you, you do not need to send a password in this field. Instead, you could pass another authentication token, such as a Kerberos Ticket so that your actual corporate passwords are not passed to or from Salesforce.

      You can configure the Salesforce delegated authentication authority to allow only tokens or to accept either tokens or passwords. If the authority only accepts tokens, a Salesforce user cannot log in to Salesforce directly, because they cannot create a valid token. However, many companies choose to allow both tokens and passwords. In this environment, a user could still log in to Salesforce through the login page.

      When the Salesforce server passes these credentials back to you in the `Authenticate` message, verify them, and the user will gain access to the application.

3. In Salesforce, specify your organization's single sign-on gateway URL from Setup by entering *`Single Sign-On`* in the `Quick Find` box, selecting **Single Sign-On Settings**, then clicking **Edit**. Enter the URL in the **Delegated Gateway URL** text box.

   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.

4. Optionally, check the **Force Delegated Authentication Callout** box.

   Note: When this box is unchecked, a call is not made to the SSO endpoint if the login attempt first fails because of login restrictions within the Salesforce organization. If you must record every login attempt, then check this box to force a callout to the SSO endpoint regardless of login restriction failures.

5. Enable the "Is Single Sign-On Enabled" permission.

Important: If single sign-on 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. Furthermore, the single sign-on authority usually handles login lockout policies for users with the "Is Single Sign-On Enabled" permission. However, if the security token is enabled

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"

for your org, then 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

Understanding Delegated Authentication Single Sign-On

Control Individual API Client Access to Your Salesforce Organization

With API Client Whitelisting, restrict all API client applications, such as the Data Loader, to require administrator approval, unless the user's profile or permission set has the "Use Any API Client" permission.

Administrators may grant some users API access through the "API Enabled" permission. After it's given, this permission allows the user API access through any client (such as the Data Loader, Salesforce1, Salesforce for Outlook, or the Force.com Migration Tool). For finer control over which applications the user can use for API access, you can implement API Client Whitelisting. This feature leverages the existing authorization capabilities of connected apps. With API Client Whitelisting, an administrator can approve or block individual client application access for each associated connected app. All client applications that are not configured as connected apps are denied access. If you are not using connected apps, you can relax this restriction for individual users by assigning them a profile or permission set with "Use Any API Client" enabled.

Note: Contact Salesforce to enable API Client Whitelisting. After it's enabled, all client access is restricted until explicitly allowed by the administrator. This restriction might block access to applications that your users are already using. Before you enable this feature, you should configure and approve connected apps for any client applications you want users to continue using, or give the users a profile or permission set with "Use Any API Client" enabled.

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"

To configure API Client Whitelisting, do the following.

1. Contact Salesforce to get the feature enabled for your organization.
2. From Setup, enter *Connected Apps* in the `Quick Find` box, then select the option for managing connected apps.
3. In the App Access Settings, click **Edit**.
4. Select **Limit API access to installed connected apps with the "Admin approved users are pre-authorized" policy**.

   Optionally, select **Allow Visualforce pages to bypass this restriction** so that any Visualforce pages that use the API continue to be authorized to access objects in the organization. If you enable API Client Whitelisting without selecting this option, only approved connected apps are authorized, and Visualforce pages might not behave as expected. Also, if unchecked, client applications that call `getSessionId()` are denied access. Apps that make API calls to Salesforce using a session obtained in a Visualforce context are denied access unless you select this checkbox.
5. Click **Save**.

After you select this feature, all client applications need explicit approval by an administrator to be authorized for the organization, unless the user has a profile or permission set with "Use Any API Client" enabled.

Some components for commonly used apps are automatically installed as connected apps in organizations. These components support apps such as the Data Loader, Salesforce1, Workbench and more. After you select this feature, these components will also require approval, unless the user has a profile or permission set with "Use Any API Client" enabled. See Managing a Connected App for more information about these components.

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.

Note: Contact Salesforce to learn more about enabling Single Sign-On for your organization.

USER PERMISSIONS

To view Single Sign-On login errors:
- "Modify All Data"

SEE ALSO:

Single Sign-On

About SAML

Security Assertion Markup Language (SAML) is an XML-based standard that allows you to communicate authentication decisions between one service and another. It underlies many Web single sign-on solutions. Salesforce supports SAML for single sign-on into Salesforce from a corporate portal or identity provider.

Much of the work to set up single sign-on using SAML occurs with your identity provider:

1. Establish a SAML identity provider and gather information about how they will connect to Salesforce. This is the provider that will send single sign-on 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 Configuring SAML Settings for Single Sign-On. This is the only step that takes place in Salesforce.

Your identity provider should send 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 allows single sign-on if the assertion is true.

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 may need to obtain a SAML assertion from your identity provider.

If your users are having problems using SAML to login, 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 your identity provider supports metadata, and if you've configured SAML using version 2.0, you can click **Download Metadata** to download an XML configuration file to send them, which they can then upload to automatically configure their settings for connecting to your Salesforce organization or community.

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

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.

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"

3. Share the example SAML assertions with your identity provider so they can determine the format Salesforce requires for successful single sign-on.

SEE ALSO:

About SAML

Configuring SAML Settings for Single Sign-On

From this page, you can configure your organization 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 new configuration, as follows.
   - **New** - Specify all settings manually.
   - **New from Metadata File** - Import SAML 2.0 settings from a 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 located 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 organization.

   Salesforce inserts the corresponding **API Name** value, which you can customize if necessary.

7. Enter the `Issuer`. This is often referred to as the entity ID for the identity provider.
8. If your Salesforce organization 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 organization 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 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.
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**.

If your identity provider supports metadata, and if you've configured SAML using version 2.0, you can click **Download Metadata** to download an XML configuration file to send them, which they can then upload to automatically configure their settings for connecting to your Salesforce organization or community.

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 (this applies to organizations created before the Summer '13 release that are not 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 organization'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 may be unable 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 may have to obtain a SAML assertion from your identity provider first.

If your users are having problems using SAML to login, 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 this with the Web single sign-on authentication flow for OAuth 2.0.

SEE ALSO:

- About SAML
- Best Practices for Implementing Single Sign-On
- Validating SAML Settings for Single Sign-On
- Administrator setup guide: Single Sign-On Implementation Guide
- About Salesforce Certificates and Keys

Viewing Single Sign-On Settings

After you have configured your Salesforce organization to use SAML, you can view the single sign-on settings. From Setup, enter *Single Sign-On Settings* in the Quick Find box, then select **Single Sign-On Settings**.

This page lists the details of your SAML configuration. Most of these fields are the same as the fields on the page where you configured SAML. The following fields contain information automatically generated by completing the configuration. The available fields depend on your configuration.

Field	Description
Salesforce Login URL	For SAML 2.0 only. If you select "Assertion contains User's Salesforce username" for SAML User ID Type and "User ID is in the NameIdentifier element of the Subject statement" for SAML User ID Location, this URL is the URL associated with login for the Web single sign-on OAuth assertion flow.
Salesforce Logout URL	For SAML 2.0. Displays the Salesforce logout URL that the user is directed to after he or she logs off. This URL is only used if no value is specified for Identity Provider Logout URL.
OAuth 2.0 Token Endpoint	For SAML 2.0 only: The ACS URL used with enabling Salesforce as an identity provider in the Web single sign-on 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 organization using a SAML assertion provided by your identity provider.
- If your identity provider supports metadata, and if you've configured SAML using version 2.0, you can click **Download Metadata** to download an XML configuration file to send them, which they can then upload to automatically configure their settings for connecting to your Salesforce organization or community.

SEE ALSO:

About 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://na1.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:

About 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://na1.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.

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.

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:

About 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:

About 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:

About 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:

- About 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:

About 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:

SEE ALSO:

Just-in-Time Provisioning Requirements

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.

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 for Portals

Just-in-Time Provisioning for Communities

"Configuring SAML for Communities" in Getting Started With Communities

Just-in-Time Provisioning 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.

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.

Fields	Required	Comments
IsCustomerPortal		
IsPartner		
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		

Fields	Required	Comments
Phone		
Salutation		
Title		

SEE ALSO:

- About Just-in-Time Provisioning for SAML
- Just-in-Time Provisioning Requirements
- Just-in-Time Provisioning for Communities
- "Configuring SAML for Communities" in Getting Started With 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 Configuring 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 under the specified `Account ID` (`Contact.Account` or `Account.AccountNumber`) for a match based on the Contact ID (`User.ContactId`) or email (`Contact.Email`).
     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 both the `Account.AccountNumber` and `Account.Name` specified in the SAML assertion, or updates the existing contact and user records for the account if a match is found..
        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 a new account record, inserts a new contact record, and inserts a new user record 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

Fields	Required	Comments
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		
Title		

SEE ALSO:

- About Just-in-Time Provisioning for SAML
- Just-in-Time Provisioning Requirements
- "Configuring SAML for Communities" in Getting Started With Communities

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
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

Code	Description	Error Details
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
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 for Portals

About External Authentication Providers

You can enable users to log into your Salesforce organization using their login credentials from an external service provider such as Facebook© or Janrain©.

Note: Social Sign-On (11:33 minutes)

Learn how to configure single sign-on and OAuth-based API access to Salesforce from other sources of user identity.

Do the following to successfully set up an authentication provider for single sign-on.

- Correctly configure the service provider website.
- Create a registration handler using Apex.
- Define the authentication provider in your organization.

When set up is complete, the authentication provider flow is as follows.

1. The user tries to login to Salesforce using a third party identity.
2. The login request is redirected to the third party authentication provider.
3. The user follows the third party login process and approves access.
4. The third party authentication provider redirects the user to Salesforce with credentials.
5. The user is signed into Salesforce.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

  "Manage Auth. Providers"

Note: If a user has an existing Salesforce session, after authentication with the third party they are automatically redirected to the page where they can approve the link to their Salesforce account.

Defining Your Authentication Provider

We support the following providers:

- Facebook
- Google
- Janrain
- LinkedIn
- Microsoft Access Control Service
- Salesforce
- Twitter
- Any service provider who implements the OpenID Connect protocol

Adding 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 656 – Sends the user to a specific endpoint for authentication (Salesforce authentication providers, only)

Creating an Apex Registration Handler

A registration handler class is required to use Authentication Providers for the single sign-on flow. 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:

Configuring a Facebook Authentication Provider

Configure a Google Authentication Provider

Let users log in to a Salesforce organization using their Google accounts.

Configure a Janrain Authentication Provider

Configure a Salesforce Authentication Provider

Configure an OpenID Connect Authentication Provider

You can use any third-party Web application 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

Let users log in to a Salesforce organization using their LinkedIn account.

Configure a Twitter Authentication Provider

Let users log in to a Salesforce organization with their Twitter accounts.

Using Salesforce-Managed Values in Auth. Provider Setup

You can choose to let Salesforce automatically create key values when setting up a Facebook, Salesforce, LinkedIn, Twitter, or Google Auth. Provider. This allows you to skip the step of creating your own third-party application.

Create a Custom External Authentication Provider

Create a single sign-on (SSO) authentication provider to let admins and users use their non-Salesforce SSO credentials for your Salesforce orgs.

Configuring a Facebook Authentication Provider

To use Facebook as an authentication provider:

1. Set up a Facebook application, making Salesforce the application domain.
2. Define a Facebook authentication provider in your Salesforce organization.
3. Update your Facebook application to use the `Callback URL` generated by Salesforce as the Facebook `Website Site URL`.
4. Test the connection.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

  "Manage Auth. Providers"

Setting up a Facebook Application

Before you can configure Facebook for your Salesforce organization, you must set up an application in Facebook:

Note: You can skip this step by allowing Salesforce to use its own default application. For more information, see Using Salesforce-Managed Values in Auth. Provider Setup.

1. Go to the Facebook website and create a new application.
2. Modify the application settings and set the Application Domain to Salesforce.
3. Note the Application ID and the Application Secret.

Defining a Facebook Provider in your Salesforce Organization

You need the Facebook Application ID and Application Secret to set up a Facebook provider in your Salesforce organization.

Note: You can skip specifying these key values in the provider setup by allowing Salesforce to manage the values for you. For more information, see Using Salesforce-Managed Values in Auth. Provider Setup.

1. From Setup, enter *`Auth. Providers`* in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. Select Facebook for the `Provider Type`.
4. Enter a `Name` for the provider.

5. Enter the `URL Suffix`. This is used in the client configuration URLs. For example, if the URL suffix of your provider is "MyFacebookProvider", your single sign-on URL is similar to: `https://login.salesforce.com/auth/sso/00Dx00000000001/MyFacebookProvider`.
6. Use the Application ID from Facebook for the `Consumer Key` field.
7. Use the Application Secret from Facebook 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 application uses.

      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`. In this example, the additional `approval_prompt` parameter is necessary to ask the user to accept the refresh action, so that Google 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 application 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 requested scopes. If you leave this field blank, Salesforce uses the version of the Facebook API that your application 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 Using 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 single sign-on 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 already 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. You must edit this class and modify the default content before using it.

      Note: You must specify a registration handler class for Salesforce to generate the `Single Sign-On Initialization URL`.

   h. Select the user that runs the Apex handler class for **Execute Registration As**. The user must have "Manage Users" permission. A user is required if you selected a registration handler class or are automatically creating one.
   i. To use a portal with your provider, select the portal from the Portal drop-down 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, and does not appear on the login page for your Salesforce organization or custom domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

      You can specify a path to your own image, or copy the URL for one of our sample icons into the field.
9. 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`: Administrators use this URL to ensure the third-party provider is set up correctly. The administrator 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 into Salesforce from a third party (using third-party credentials). The end user opens this URL in a browser, and signs in to the third party. This then either creates a new user for them, or updates an existing user, and then signs them into Salesforce as that user.
- `Existing User Linking URL`: Use this URL to link existing Salesforce users to a third-party account. The end 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 single sign-on 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 of the above client configuration URLs.

The client configuration URLs support additional request parameters that enable you to direct users to log into specific sites, obtain customized permissions from the third party, or go to a specific location after authenticating.

Updating Your Facebook Application

After defining the Facebook authentication provider in your Salesforce organization, go back to Facebook and update your application to use the `Callback URL` as the Facebook `Website Site URL`.

Testing the Single Sign-On Connection

In a browser, open the `Test-Only Initialization URL` on the Auth. Provider detail page. It should redirect you to Facebook and ask you to sign in. Upon doing so, you are asked to authorize your application. After you authorize, you are redirected back to Salesforce.

SEE ALSO:

Using Request Parameters with Client Configuration URLs

About External Authentication Providers

Configure a Google Authentication Provider

Let users log in to a Salesforce organization using their Google accounts.

To use Google as an authentication provider:

1. Set up a Google application, making Salesforce the application domain.
2. Define a Google authentication provider in your Salesforce organization.
3. Update your Google application 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: **Professional**, **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 Application

Before you can configure Google for your Salesforce organization, you must set up an application in Google:

Note: You can skip this step by allowing Salesforce to use its own default application. For more information, see Using Salesforce-Managed Values in Auth. Provider Setup.

1. Go to the Google website and create a new application.
2. Modify the application settings and set the Application Domain to Salesforce.
3. Note the Application ID and the Application Secret.

Define a Google Provider in Your Salesforce Organization

You need the Google Application ID and Application Secret to set up a Google provider in your Salesforce organization.

Note: You can skip specifying these key values in the provider setup by allowing Salesforce to manage the values for you. For more information, see Using Salesforce-Managed Values in Auth. Provider Setup.

1. From Setup, enter *`Auth. Providers`* in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. Select Google for the `Provider Type`.
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 single sign-on URL is similar to: `https://login.salesforce.com/auth/sso/00Dx00000000001/MyGoogleProvider`.
6. Use the Application ID from Google for the `Consumer Key` field.
7. Use the Application Secret from Google for the `Consumer Secret` field.
8. Optionally, set the following fields.
   a. `Authorize Endpoint URL` to 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`.

The `approval_prompt` parameter is necessary 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` to 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` to change the values requested from Google's profile API. The URL must start with *`https://www.googleapis.com/oauth2/`*.

d. `Default Scopes` to 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 Using the Scope Parameter.

e. `Custom Error URL` to 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 single sign-on 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. To create an Apex class template for the registration handler, select an existing Apex class as the `Registration Handler` class or click `Automatically create a registration handler template`. Edit this class and modify the default content before using it.

Note: Specify a registration handler class for Salesforce to generate the `Single Sign-On Initialization URL`.

h. Select the user that runs the Apex handler class for **Execute Registration As**. The user must have "Manage Users" permission. You must specify a user if you selected a registration handler class or are automatically creating one.

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, and does not appear on the login page for your Salesforce organization or custom domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

You can 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`: Administrators use this URL to ensure that the third-party provider is set up correctly. The administrator 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 into Salesforce from a third party (using third-party credentials). The end user opens this URL in a browser and signs in to the third party. The third party then either creates a user or updates an existing user, and then signs them into Salesforce as that user.
- `Existing User Linking URL`: Use this URL to link existing Salesforce users to a third-party account. The end 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 single sign-on 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.

The 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 Application

After defining the Google authentication provider in your Salesforce organization, go back to Google and update your application to use the `Callback URL` as the Google `Website Site URL`.

Test the Single Sign-On Connection

In a browser, open the `Test-Only Initialization URL` on the Auth. Provider detail page. It redirects you to Google and asks you to sign in. You're then asked to authorize your application. After you authorize, you're redirected to Salesforce.

Configure a Janrain Authentication Provider

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 application with Janrain and get an `apiKey`.
2. Define the Janrain authentication provider in your Salesforce organization.
3. Get the login widget code from Janrain.
4. Set up a site that calls the login widget code in your Salesforce organization.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

  "Manage Auth. Providers"

Register Your Application

You must sign up for a Janrain account from the Janrain website. Once you have your Janrain account, you need the `apiKey`.

1. Click **Deployment** > **Sign-in for Web** > **Handle Tokens**.
2. Copy the `apiKey`. You need this when creating the Janrain provider in your Salesforce organization.
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 Organization

You need the Janrain `apiKey` to create a Janrain provider in your Salesforce organization.

1. From Setup, enter *`Auth. Providers`* in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. Select Janrain for the `Provider Type`.
4. Enter a `Name` for the provider.
5. Enter the `URL Suffix`. This 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 any errors.
8. Optionally, enter a `Custom Logout URL` to provide a specific destination for users after they log out, if they authenticated using the single sign-on 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 already existing Apex class as the `Registration Handler` class or click `Automatically create a registration handler template` to create the Apex class template for the registration handler. You must edit this class to modify the default content before using it.

   Note: You must specify a registration handler class for Salesforce to use single sign-on.

10. Select the user that runs the Apex handler class for **Execute Registration As**. The user must have "Manage Users" permission. A user is required if you selected a registration handler class or are automatically creating one.
11. To use a portal with your provider, select the portal from the Portal drop-down 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, and does not appear on the login page for your Salesforce organization or custom domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

    You can 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 it to complete the Janrain setup.

Several client configuration parameters are available after configuring Janrain as the authentication provider. Use these for the `flowtype` value in the `Callback URL` with your Janrain login widget:

- `test`: Use this parameter to make sure the third-party provider is set up correctly. The administrator 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`: Use this parameter to link existing Salesforce users to a third-party account . The end 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`: Use this parameter to perform single sign-on into Salesforce from a third party (using third-party credentials). The end user goes to a page with a Janrain widget configured to use `flowtype=sso`, and signs in to the third party. This then either creates a new user for them, or updates an existing user, and then signs them into Salesforce as that user.

The client configuration URLs support additional request parameters that enable you to direct users to log into 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 organization.

1. From your Janrain account, click **Application** > **Sign-in for Web** > **Get the Code**.
2. Enter the `Callback URL` value from your Janrain provider information in your Salesforce organization 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 custom 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 new site and specify the page you just created as the home page for the site.

SEE ALSO:

- Using Request Parameters with Client Configuration URLs
- About External Authentication Providers
- "Configuring Authentication Providers" in Getting Started With Communities

Configure a Salesforce Authentication Provider

You can use a connected app as an authentication provider. You must complete these steps:

1. Define a Connected App.
2. Define the Salesforce authentication provider in your organization.
3. Test the connection.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

  "Manage Auth. Providers"

Define a Connected App

Before you can configure a Salesforce provider for your Salesforce organization, you must define a connected app that uses single sign-on. From Setup, enter *Apps* in the `Quick Find` box, then select **Apps**.

After you finish defining a connected app, save the values from the `Consumer Key` and `Consumer Secret` fields.

Note: You can skip this step by allowing Salesforce to use its own default application. For more information, see Using Salesforce-Managed Values in Auth. Provider Setup.

Define the Salesforce Authentication Provider in your Organization

You need the values from the `Consumer Key` and `Consumer Secret` fields of the connected app definition to set up the authentication provider in your organization.

Note: You can skip specifying these key values in the provider setup by allowing Salesforce to manage the values for you. For more information, see Using Salesforce-Managed Values in Auth. Provider Setup.

1. From Setup, enter *Auth. Providers* in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. Select Salesforce for the `Provider Type`.
4. Enter a `Name` for the provider.

5. Enter the `URL Suffix`. This is used in the client configuration URLs. For example, if the URL suffix of your provider is "MySFDCProvider", your single sign-on URL is similar to `https://login.salesforce.com/auth/sso/00Dx00000000001/MySFDCProvider`.
6. Paste the value of `Consumer Key` from the connected app definition into the `Consumer Key` field.
7. Paste the value of `Consumer Secret` 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://test.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://test.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 Using the Scope Parameter.

      Note: When editing the settings for an existing Salesforce authentication provider, you might have the option to select a checkbox to include the organization ID for third-party account links. For Salesforce authentication providers set up in the Summer '14 release and earlier, the user identity provided by an organization does not include the organization ID. So, the destination organization can't differentiate between users with the same user ID from two sources (such as two sandboxes). Select this checkbox if you have an existing organization with two users (one from each sandbox) mapped to the same user in the destination organization, and you want to keep the identities separate. Otherwise, leave this checkbox unselected. After enabling this feature, your users need to re-approve the linkage to all of their third party links. These links are listed in the Third-Party Account Links section of a user's detail page. Salesforce authentication providers created in the Winter '15 release and later have this setting enabled by default and do not display the checkbox.

   d. `Custom Error URL` for the provider to use to report any errors.
   e. `Custom Logout URL` to provide a specific destination for users after they log out, if they authenticated using the single sign-on 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 already existing Apex class as the `Registration Handler` class or click `Automatically create a registration handler template` to create the Apex class template for the registration handler. You must edit this template class to modify the default content before using it.

   Note: You must specify a registration handler class for Salesforce to generate the `Single Sign-On Initialization URL`.
10. Select the user that runs the Apex handler class for `Execute Registration As`. The user must have "Manage Users" permission. A user is required if you selected a registration handler class or are automatically creating one.
11. To use a portal with your provider, select the portal from the Portal drop-down 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, and does not appear on the login page for your Salesforce organization or custom domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

    You can 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, and you use the `Test-Only Initialization URL` to check your configuration. Also be sure to note the `Auth. Provider Id` value because you must use it with the `Auth.AuthToken` Apex class.

14. Return to the connected app definition that you created earlier (on the Apps page in Setup, click the connected app name) and paste the value of `Callback URL` from the authentication provider into the `Callback URL` field.

Several client configuration URLs are generated after defining the authentication provider:

- `Test-Only Initialization URL`: Administrators use this URL to ensure the third-party provider is set up correctly. The administrator 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 into Salesforce from a third party (using third-party credentials). The end user opens this URL in a browser, and signs in to the third party. This then either creates a new user for them, or updates an existing user, and then signs them into Salesforce as that user.
- `Existing User Linking URL`: Use this URL to link existing Salesforce users to a third-party account. The end 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 single sign-on 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 of the above client configuration URLs.

The client configuration URLs support additional request parameters that enable you to direct users to log into specific sites, obtain customized permissions from the third party, or go to a specific location after authenticating.

Test the Single Sign-On Connection

In a browser, open the `Test-Only Initialization URL` on the Auth. Provider detail page. Both the authorizing organization and target organization must be in the same environment, such as production or sandbox.

SEE ALSO:

Using Request Parameters with Client Configuration URLs

About External Authentication Providers

Configure an OpenID Connect Authentication Provider

You can use any third-party Web application that implements the server side of the OpenID Connect protocol, such as Amazon, Google, and PayPal, as an authentication provider.

You must complete these steps to configure an OpenID authentication provider:

1. Register your application, making Salesforce the application domain.
2. Define an OpenID Connect authentication provider in your Salesforce organization.
3. Update your application to use the `Callback URL` generated by Salesforce as the callback URL.
4. Test the connection.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

  "Manage Auth. Providers"

Register an OpenID Connect Application

Before you can configure a Web application for your Salesforce organization, 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 application on your service provider's website.
2. Modify the application settings and set the application domain (or `Home Page URL`) to Salesforce.
3. Note the Client ID and Client Secret, as well as the Authorize Endpoint URL, Token Endpoint URL, and User Info Endpoint URL, which should be available in the provider's documentation. Here are some common OpenID Connect service providers:
   - Amazon
   - Google
   - PayPal

Define an OpenID Connect Provider in Your Salesforce Organization

You need some information from your provider (the Client ID and Client Secret, as well as the Authorize Endpoint URL, Token Endpoint URL, and User Info Endpoint URL) to configure your application in your Salesforce organization.

1. From Setup, enter *`Auth. Providers`* in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. Select OpenID Connect for the `Provider Type`.
4. Enter a `Name` for the provider.
5. Enter the `URL Suffix`. This 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`.

In this specific case, the additional `approval_prompt` parameter is necessary to ask the user to accept the refresh action, so Google will continue 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 is not 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 Using the Scope Parameter.

11. You can 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 single sign-on 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. You must edit this class and modify the default content before using it.

    Note: You must specify a registration handler class for Salesforce to generate the `Single Sign-On Initialization URL`.

    d. Select the user that runs the Apex handler class for **Execute Registration As**. The user must have the "Manage Users" permission. A user is required if you selected a registration handler class or are automatically creating one.
    e. To use a portal with your provider, select the portal from the Portal drop-down 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, and does not appear on the login page for your Salesforce organization or custom domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

    You can 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`: Administrators use this URL to ensure the third-party provider is set up correctly. The administrator 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 into Salesforce from a third party (using third-party credentials). The end user opens this URL in a browser, and signs in to the third party. This then either creates a new user for them, or updates an existing user, and then signs them into Salesforce as that user.
- `Existing User Linking URL`: Use this URL to link existing Salesforce users to a third-party account. The end 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 single sign-on 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 of the above client configuration URLs.

The client configuration URLs support additional request parameters that enable you to direct users to log into specific sites, obtain customized permissions from the third party, or go to a specific location after authenticating.

Update Your OpenID Connect Application

After defining the authentication provider in your Salesforce organization, go back to your provider and update your application's `Callback URL` (also called the `Authorized Redirect URI` for Google applications and `Return URL` for PayPal).

Test the Single Sign-On Connection

In a browser, open the `Test-Only Initialization URL` on the Auth. Provider detail page. It should redirect you to your provider's service and ask you to sign in. Upon doing so, you're asked to authorize your application. 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 authentication from a Microsoft authentication provider is not supported.

You must complete these steps to configure a Microsoft Access Control Service authentication provider:

1. Define a Microsoft Access Control Service authentication provider in your Salesforce organization.
2. Register your application 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 application with Microsoft.
4. Test the connection.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

  "Manage Auth. Providers"

Define a Microsoft Access Control Service Authentication Provider in Your Salesforce Organization

Before you can register an application in SharePoint Online or the Microsoft Seller Dashboard, you need the callback URL that will be used to redirect the authorized user to Salesforce.

1. From Setup, enter *`Auth. Providers`* in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. Select Microsoft Access Control Service for the `Provider Type`.
4. Enter a `Name` for the provider.
5. Enter the `URL Suffix`. This 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'll edit this value after your application is registered with Microsoft).
7. Enter a placeholder value for the `Consumer Secret` field (you'll edit this value after your application 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 Using 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 single sign-on 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` drop-down list. If you have a portal set up for your organization, 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, and does not appear on the login page for your Salesforce organization or custom domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

      You can specify a path to your own image, or copy the URL for one of our sample icons into the field.

11. Click **Save**.

Be sure to 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`: Administrators use this URL to ensure the third-party provider is set up correctly. The administrator 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 does not provide for future single sign-on 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 of the above client configuration URLs.

The client configuration URLs support additional request parameters that enable you to direct users to log into specific sites, obtain customized permissions from the third party, or go to a specific location after authenticating.

Register Your Application with Microsoft

Before you can configure an application for your Salesforce organization, you must get an application identity using one of the options provided by Microsoft. For example see Guidelines for registering apps for SharePoint 2013 for details about registering a remote application for SharePoint.

1. Register your application using one of the options provided by Microsoft.
2. Modify the application 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 application 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. Enter the `Client ID` value provided by Microsoft in the `Consumer Key` field.
4. Enter the `Client Secret` value provided by Microsoft in the `Consumer Secret` field.

Test the Connection

In a browser, open the `Test-Only Initialization URL` on the Auth. Provider detail page. It should redirect you to your provider's service and ask you to sign in. Upon doing so, you're asked to authorize your application. After you authorize, you're redirected back to Salesforce.

Configure a LinkedIn Authentication Provider

Let users log in to a Salesforce organization using their LinkedIn account.

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 application.
3. Define a LinkedIn Provider in your Salesforce organization and establish a registration handler.
4. Edit the registration handler.
5. Update your LinkedIn application 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 connection.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

  "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 some basic information, such as username and a photo URL, or you can get more specific information, such as an address, phone number, contact list, and more. The user approves the exchange of information before it is given.

When you set up LinkedIn as an Auth. Provider, you can set the scopes in three different places: in the LinkedIn application 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 this 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 Auth. Provider settings, that value overrides the value in the LinkedIn Application settings.
- Separate multiple scope values in the LinkedIn Application settings or the Salesforce Auth. Provider settings with a space, only, such as `r_basicprofile r_emailaddress`.
- If you use LinkedIn Field Selectors with a URL, separate multiple values with a comma, only, such as `https://api.linkedin.com/v1/people/~:(id,formatted-name,first-name,last-name,public-profile-url,email-address)`.

Set up a LinkedIn application

Before you can configure LinkedIn for your Salesforce organization, set up an application in LinkedIn.

Note: You can skip this step by allowing Salesforce to use its own default application. For more information, see Using Salesforce-Managed Values in Auth. Provider Setup.

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 application settings.

5. Note the API Key and Secret Key of the new application. You need these later in Salesforce.
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 organization

You need the LinkedIn `API Key` and `Secret Key` to set up a LinkedIn provider in your Salesforce organization.

Note: You can skip specifying these key values in the provider setup by allowing Salesforce to manage the values for you. For more information, see Using Salesforce-Managed Values in Auth. Provider Setup.

1. From Setup, enter *`Auth. Providers`* in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. Select LinkedIn for the `Provider Type`.
4. Enter a `Name` for the provider.
5. Enter the `URL Suffix`. This is used in the client configuration URLs. For example, if the URL suffix of your provider is "MyLinkedInProvider," your single sign-on URL is similar to:

   `https://login.salesforce.com/services/sso/00Dx00000000001/MyLinkedInProvider`
6. Use the `API Key` from LinkedIn for the `Consumer Key` field.
7. Use the `Secret Key` from LinkedIn 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 Google for offline access, use `https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force`. The `approval_prompt` parameter is necessary 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` 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 single sign-on 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. Click **Automatically create a registration handler template** to create an Apex class template for the registration handler, unless you already have one. Edit this class later, and modify the default content before using it.

Note: Specify a registration handler class for Salesforce to generate the Single Sign-On Initialization URL.

h. Select the user that runs the Apex handler class for `Execute Registration As`. The user must have the "Manage Users" permission. A user is required if you selected a registration handler class or are automatically creating one.

i. To use a portal for LinkedIn users, select the portal from the Portal drop-down 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, and does not appear on the login page for your Salesforce organization or custom domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

   You can 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`: Administrators use this URL to ensure the third-party provider is set up correctly. The administrator 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 into Salesforce from a third party (using third-party credentials). The end user opens this URL in a browser, and signs in to the third party. This then either creates a new user for them, or updates an existing user, and then signs them into Salesforce as that user.
- `Existing User Linking URL`: Use this URL to link existing Salesforce users to a third-party account. The end 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 single sign-on 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 of the above client configuration URLs.

The client configuration URLs support additional request parameters that enable you to direct users to log into 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.

   The following is an example Apex registration handler specifically for a LinkedIn application as the Auth. Provider. This registration handler assumes the requested scopes include *`r_basicprofile`* and *`r_emailaddress`*. It also assumes 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 Application

After you define the LinkedIn authentication provider in your Salesforce organization, go back to LinkedIn and update your application to use the Salesforce-generated `Callback URL` as the LinkedIn `OAuth 2.0 Redirect URLs` value.

Test the Single Sign-on Connection

In a browser, open the `Test-Only Initialization URL` on the Auth. Provider detail page. It should redirect you to LinkedIn and ask you to sign in. Upon doing so, you are asked to authorize your application. After you authorize, you are redirected back to Salesforce.

Configure a Twitter Authentication Provider

Let users log in to a Salesforce organization with their Twitter accounts.

Complete these steps to configure Twitter as an authentication provider.

1. Set up a Twitter application.
2. Define a Twitter Provider in your Salesforce organization and establish a registration handler.
3. Edit the registration handler.
4. Update your Twitter application to use the Callback URL generated by Salesforce as an entry in the Twitter application settings.
5. Test the single sign-on connection.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

  "Manage Auth. Providers"

Set up a Twitter Application

Before you can configure Twitter for your Salesforce organization, you must set up an application in Twitter.

Note: You can skip this step by allowing Salesforce to use its own default application. For more information, see Using Salesforce-Managed Values in Auth. Provider Setup.

1. Sign in to your developer account for the Twitter website.
2. Click on the user icon at the top and select **My Applications** (or go to apps.twitter.com).
3. Click **Create New App**.
4. Enter the application settings.

5. In the API Keys, note the `API key` and `API secret` of the new application, you'll need these later in Salesforce.

Define a Twitter Provider in your Salesforce organization

You need the Twitter `API key` and `API Secret` from your Twitter application to set up a Twitter provider in your Salesforce organization.

Note: You can skip specifying these key values in the provider setup by allowing Salesforce to manage the values for you. For more information, see Using Salesforce-Managed Values in Auth. Provider Setup.

1. From Setup, enter *`Auth. Providers`* in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. Select Twitter for the `Provider Type`.
4. Enter a `Name` for the provider.
5. Enter the `URL Suffix`. This is used in the client configuration URLs. For example, if the URL suffix of your provider is "MyTwitterProvider," your single sign-on 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 single sign-on 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. Click **Automatically create a registration handler template** to create an Apex class template for the registration handler, unless you already have one. You must edit this class, later, and modify the default content before using it.

      Note: You must specify a registration handler class for Salesforce to generate the Single Sign-On Initialization URL.

   d. Select the user that runs the Apex handler class for `Execute Registration As`. The user must have the "Manage Users" permission. A user is required if you selected a registration handler class or are automatically creating one.
   e. To use a portal for Twitter users, select the portal from the Portal drop-down 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, and does not appear on the login page for your Salesforce organization or custom domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

      You can 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`: Administrators use this URL to ensure the third-party provider is set up correctly. The administrator 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 into Salesforce from a third party (using third-party credentials). The end user opens this URL in a browser, and signs in to the third party. This then either creates a new user for them, or updates an existing user, and then signs them into Salesforce as that user.

- `Existing User Linking URL`: Use this URL to link existing Salesforce users to a third-party account. The end 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 of the above client configuration URLs.

The client configuration URLs support additional request parameters that enable you to direct users to log into 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.

   The following is an example Apex registration handler specifically for a Twitter application as the Auth. 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 Application

After you define the Twitter authentication provider in your Salesforce organization, go back to Twitter and update your application to use the Salesforce-generated `Callback URL` as the `Callback URL` value in your Twitter application settings.

Note: In your Twitter application, make sure that you select **Allow this application to be used to Sign In with Twitter**.

Test the Single Sign-on Connection

In a browser, open the `Test-Only Initialization URL` on the Auth. Provider detail page. It should redirect you to Twitter and ask you to sign in. Upon doing so, you are asked to authorize your application. After you authorize, you are redirected back to Salesforce.

Using Salesforce-Managed Values in Auth. Provider Setup

You can choose to let Salesforce automatically create key values when setting up a Facebook, Salesforce, LinkedIn, Twitter, or Google Auth. Provider. This allows you to skip the step of creating your own third-party application.

When you choose to use Salesforce-managed values in your Auth. Provider setup, Salesforce uses its own default application in the background from which it generates the values, eliminating the need for you to create your own application.

To use Salesforce-managed values, leave all of the following fields blank if they display in your Auth. Provider setup.

- `Consumer Key`
- `Consumer Secret`
- `Authorize Endpoint URL`
- `Token Endpoint URL`
- `User Info Endpoint URL`
- `Default Scopes`

If you specify a value for one of the preceding fields, then that indicates that you are using your own third-party application or connected app and you must specify values for the `Consumer Key` and `Consumer Secret`.

Example: Suppose you want to set up single sign-on using a LinkedIn authentication provider to enable login to Salesforce with LinkedIn credentials. You can skip creating a LinkedIn application, since you choose to use Salesforce-created values in Auth. Provider setup. Next, you define the LinkedIn authentication provider in your organization and test the connection using the procedure in Configure a LinkedIn Authentication Provider.

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

  "Manage Auth. Providers"

Create a Custom External Authentication Provider

Create a single sign-on (SSO) authentication provider to let admins and users use their non-Salesforce SSO credentials for your Salesforce orgs.

1. Set up an account with your chosen 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, and use these classes to implement the `Auth.AuthProviderPlugin` interface.
4. Configure your new metadata through the Auth Provider Setup page.
5. Update your application to use the Callback URL generated by Salesforce.
6. Test the connection.

EDITIONS

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

Set up Your Account

Before you can configure the auth provider plug-in for your Salesforce org, set up an account with your chosen external auth provider.

1. Go to your provider's site and create an application.
2. Modify the application settings, and set the Application Domain to Salesforce.
3. Note the application ID and application secret, if required by your external auth provider.

Create Your Custom Metadata Types

When you have an account, create the custom metadata types for your Salesforce org required by your external auth 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 and your auth provider require. For example, if the auth provider requires an application ID or application secret, you can create fields with labels like "Consumer Key" or "Consumer Secret."

Note: You are 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 auth provider for SSO, create a class that implements the `Auth.AuthProviderPlugin` interface. This interface allows you to store the custom configuration for your auth provider and handle its authentication protocols. It also creates the name for your external auth provider, and displays this name in the list of available auth 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. Implement the `Auth.AuthProviderPlugin` interface.
   b. Enter the API Name listed on your newly created custom metadata for the `return` string for the `getCustomMetadataType` method.

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 Auth Provider

You need your auth provider's application ID and application 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 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. To create an Apex class template for the registration handler, click **Automatically create a registration handler template**. Edit the class template later, and modify the default content before using it.

   Note: Specify a registration handler class for Salesforce to generate the Single Sign-On Initialization URL.

8. In the Execute Registration As field, select a user to run the Apex handler class. The user must have the "Manage Users" permission. This field is required for all custom auth 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, and does not appear on the login page for your Salesforce organization or custom domain created with My Domain. Users click the button to log in with the associated authentication provider for the community.

   You can 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 Auth Provider Id value. You use it with the `Auth.AuthToken` Apex class.

Several client configuration URLs are generated after defining the auth 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 end user opens this URL in a browser and signs in to the third party. The third party then either creates a user or updates an existing user, and then signs that user into Salesforce.
- `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.

The 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.

Updating Your External Auth Provider

After defining your authentication provider in your Salesforce org, go back to your external authentication provider's site and update your application to use the `Callback URL` as your custom auth provider's `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 your provider's site and asks you to sign in. You're then asked to authorize your application. After you authorize, you're redirected to Salesforce.

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 or other API integration, using their existing session ID and the server URL.

To authenticate users with frontdoor.jsp, you must pass the server URL and full session ID (not just the 15 or 18 character ID) to frontdoor.jsp.

The best way to pass the values is through a form that uses a `POST` request. For example, the following form posts the current session ID to frontdoor.jsp.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

```
<form method="POST" action="https://instance.salesforce.com/secur/frontdoor.jsp">
<input type="hidden" name="sid"
      value="full_sessionID_value"
      />
<input type="submit" name="login" value="Log In" /></form>
```

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://instance.salesforce.com/secur/frontdoor.jsp?sid=full_sessionID_value
&retURL=optional_relative_url_to_open
```

For organizations that use a custom domain created using My Domain, you must pass the domain name in the server URL.

The following form posts the current session ID to frontdoor.jsp for a custom domain.

```
<form method="POST" action="https://domain_name.my.salesforce.com/secur/frontdoor.jsp">
<input type="hidden" name="sid"
      value="full_sessionID_value"
      />
<input type="submit" name="login" value="Log In" /></form>
```

The following example sends the values as URL parameters.

```
https://domain_name.my.salesforce.com/secur/frontdoor.jsp?sid=full_sessionID_value
&retURL=optional_relative_url_to_open
```

Instance

You must know the instance of the user's organization. For example, if the `serverUrl` returned when you log in via the API is `https://na1.salesforce.com`, na1 is the instance. The rest of the server address (the `salesforce.com` domain name) remains the same.

If you're building an integration for a single Salesforce organization, you can hard code this value. If you're building an integration for multiple organizations, parse the instance from the `serverUrl` of the returned `LoginResult` from the SOAP API `login()` call.

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 `LoginResult` returned from a SOAP API `login()` call
- 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`).

Using Request Parameters with Client Configuration URLs

You can add functionality to your authentication provider by using additional request parameters.

Authentication providers support additional request parameters you can use to direct users to log into specific sites, obtain customized permissions from the third party, or go to a specific location after authenticating.

Add the request parameters to the following client configuration URLs. These were 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 656 – Sends the user to a specific endpoint for authentication (Salesforce authentication providers, only)

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

  "Manage Auth. Providers"

IN THIS SECTION:

Using the Scope Parameter

Customizes the permissions requested from the third party like Facebook or Janrain so that the returned access token has additional permissions.

Using the Site Parameter

Use your authentication provider to log into a site or link to a sites user.

Using the StartURL Parameter

Send your user to a specific location after authenticating or linking.

Using the Community URL Parameter

Send your user to a specific Community after authenticating.

Using the Authorization Endpoint Parameter

Send your user to a specific authorization endpoint.

Using the Scope Parameter

Customizes the permissions requested from the third party like Facebook or Janrain so that the returned access token has additional permissions.

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:

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

  "Manage Auth. Providers"

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`.

Value	Description
`visualforce`	Allows access to Visualforce pages.
`web`	Allows the ability to use the `access_token` on the Web. This also includes `visualforce`, allowing access to Visualforce pages.

SEE ALSO:

Using 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).

SEE ALSO:

Using Request Parameters with Client Configuration URLs

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

  "Manage Auth. Providers"

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=%2F005x000000000001%3Fnoredirect%3D1`

SEE ALSO:

Using Request Parameters with Client Configuration URLs

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

  "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: **Professional**, **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
```

EDITIONS

Available in: Lightning Experience and Salesforce Classic

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

  "Manage Auth. Providers"

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.

About Salesforce Certificates and Keys

Note: This information applies to Classic Encryption and not to Platform Encryption.

To work with Salesforce certificates and keys, from Setup, enter *`Certificate and Key Management`* in the `Quick Find` box, then select **Certificate and Key Management**. From this page you can manage:

- Your certificates
- Authentication Certificates
- Your master encryption keys

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To create, edit, and manage certificates:
- "Customize Application"

Certificates

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 offers two types of certificates:

Self-signed
A self-signed certificate is signed by Salesforce with the SHA-256 signature algorithm. Not all external websites accept self-signed certificates.

CA-signed
A CA-signed certificate is signed by an external certificate authority (CA). Most external websites accept CA-signed certificates. You must first generate the certificate signing request to send to a CA, and then import the signed version of the certificate before you can use it.

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.

Mutual Authentication Certificates

Note: If you don't see this option on the Certificate and Key Management page, contact Salesforce to enable the feature.

Salesforce can verify if a request comes from your organization using Salesforce certificates *and* certificates via Transport Layer Security (TLS) connections from `HTTPS` clients for mutual authentication.

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.

IN THIS SECTION:

Creating Certificates and Key Pairs

Uploading Certificate Authority (CA)-Signed Certificates

Repeating an Upload of a CA-Signed Certificate

Setting Up Mutual Authentication Certificates
Use mutual authentication for your organization by creating a mutual authentication certificate.

Configuring Your API Client to Use Mutual Authentication
Enforce SSL/TLS mutual authentication.

Managing Master Encryption Keys

Editing Salesforce Certificates and Key Pairs

Viewing Salesforce Certificates and Key Pairs

SEE ALSO:

Creating Certificates and Key Pairs
Uploading Certificate Authority (CA)-Signed Certificates
Managing Master Encryption Keys
Editing Salesforce Certificates and Key Pairs
Setting Up Mutual Authentication Certificates

Creating Certificates and Key Pairs

Salesforce offers two types of certificates:

Self-signed
A self-signed certificate is signed by Salesforce with the SHA-256 signature algorithm. Not all external websites accept self-signed certificates.

CA-signed
A CA-signed certificate is signed by an external certificate authority (CA). Most external websites accept CA-signed certificates. You must first generate the certificate signing request to send to a CA, and then import the signed version of the certificate before you can use it.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To create, edit, and manage certificates:
- "Customize Application"

To create a Salesforce certificate:

1. From Setup, enter *Certificate and Key Management* in the Quick Find box, then select **Certificate and Key Management**.
2. Select either **Create Self-Signed Certificate** or **Create CA-Signed Certificate**, based on what kind of certificate your external website accepts. You can't change the type of a certificate after you've created it.
3. Enter a descriptive label for the Salesforce certificate. This name is used primarily by administrators when viewing certificates.
4. Enter the Unique Name. This name is automatically populated based on the certificate label you enter. This name can contain only underscores and alphanumeric characters, and must be unique in your organization. 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. We recommend that you use the default key size of 2048 for security reasons. Selecting 2048 generates a certificate using 2048-bit keys and is valid for two years. Selecting 1024 generates a certificate using 1024-bit keys and is valid for one year.

   Note: Once you save a Salesforce certificate, you can't change the key size.

6. If you're creating a CA-signed certificate, you must also enter the following information. These fields are joined together to generate a unique certificate.

Field	Description
Common Name	The fully qualified domain name of the company requesting the signed certificate. This is generally of the form: http://www.mycompany.com.
Email Address	The email address associated with this certificate.

Field	Description
`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**.

Downloaded self-signed certificates have `.crt` extensions. Downloaded certificate signing requests have `.csr` extensions.

After you successfully save a Salesforce certificate, the certificate and corresponding keys are automatically generated.

You can have a maximum of 50 certificates.

After you create a CA-signed certificate, you must upload the signed certificate before you can use it.

Note: After you create a CA-signed certificate and certificate request, the certificate is not active and you can't use it until it's been signed by a certificate authority and uploaded into your organization.

SEE ALSO:

About Salesforce Certificates and Keys

Uploading Certificate Authority (CA)-Signed Certificates

Repeating an Upload of a CA-Signed Certificate

Uploading Certificate Authority (CA)-Signed Certificates

After you create a CA-signed certificate, you must do the following before the certificate is active and you can use the certificate.

1. From Setup, enter *Certificate and Key Management* in the `Quick Find` box, then select **Certificate and Key Management**, click the name of the certificate, then click **Download Certificate Signing Request**.
2. Send the certificate request to the certificate authority of your choice.
3. After the certificate authority sends back the signed certificate, from Setup, enter *Certificate and Key Management* in the `Quick Find` box, then select **Certificate and Key Management**, click the name of the certificate, then click **Upload Signed Certificate**.
4. Click **Browse** to locate the CA-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.
5. Click **Save** to finish the upload process. Click **Cancel** at any time to not upload the certificate.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To create, edit, and manage certificates:

- "Customize Application"

After you successfully upload the signed certificate, the status of the certificate is changed to `Active` and you can use CA-signed certificate.

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:

About Salesforce Certificates and Keys

Repeating an Upload of a CA-Signed Certificate

Repeating an Upload of a CA-Signed Certificate

If you upload a CA-signed certificate and either forget to upload complete certificate information or need to upload a renewed certificate, you can upload it again to finish the process. This saves you time because you don't need to start over with a new key and certificate. When you upload again, published site domains are automatically republished if they have at least one Force.com site or community. Additionally, the expiration date of the certificate record is updated to the expiration date of the newly uploaded certificate.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To create, edit, and manage certificates:

- "Customize Application"

To upload a CA-signed certificate again:

1. From Setup, enter *Certificate and Key Management* in the Quick Find box, then select **Certificate and Key Management**.
2. Click on the name of the CA-Signed certificate that you want to upload again.

   Note: Your certificate should have a `.crt` extension.

3. Click **Update Signed Certificate** and **Choose File**.
4. Click **Browse** to locate the CA-signed certificate. The CA-signed certificate's public key must match the public key of the certificate record created in Salesforce. If you try to upload a different CA-signed certificate, the upload fails.

   Note: You can click **Cancel** at any time to cancel the upload.

5. Click **Save** to finish the upload process.

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:

About Salesforce Certificates and Keys

Uploading Certificate Authority (CA)-Signed Certificates

Setting Up Mutual Authentication Certificates

Use mutual authentication for your organization by creating a mutual authentication certificate.

Note: If you don't see this option on the Certificate and Key Management page, contact Salesforce to enable the feature.

Follow these steps to upload a certificate.

1. Click **Upload Mutual Authentication Certificate**.
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.

Note that the client certificate must include any intermediate certificates in the certificate 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.

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"

SEE ALSO:

About Salesforce Certificates and Keys

Configuring Your API Client to Use Mutual Authentication

Configuring Your API Client to Use Mutual Authentication

Enforce SSL/TLS mutual authentication.

Setting Up Mutual Authentication Certificates steps should be completed before configuring your API client.

1. Log in to the Salesforce service using port 8443. Include:
   a. Your credentials
   b. 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://na1.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://na1.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.

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"

SEE ALSO:

About Salesforce Certificates and Keys

Setting Up Mutual Authentication Certificates

Managing Master Encryption Keys

Note: This information applies to Classic Encryption and not to Platform Encryption.

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 do the following:

- 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:

1. From Setup, enter *Certificate and Key Management* in the Quick Find box, then select **Certificate and Key Management**.
2. Click **Archive Current Key and Create New Key**.
3. A warning message displays letting you know you are changing keys. Click **OK**.
4. 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. You can import the key back into your organization at a later time.

Click Export next to the key you want to export.

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. If you export the key before you delete it, you can import the key back into your organization.

To delete a key, click Delete next to the key you want to delete.

The date the key is deleted displays.

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.

SEE ALSO:

About Salesforce Certificates and Keys

Editing Salesforce Certificates and Key Pairs

After you create a Salesforce certificate (including, if enabled, mutual authentication certificates) you can only change the `Label` and the `Unique Name`. You can't change the type, key size, or other properties. The certificate and the keys aren't regenerated when you edit a Salesforce certificate.

Warning: Apex and the Force.com Web services API use the `Unique Name` to access the certificate. Changing the `Unique Name` could cause your code to break.

To edit a Salesforce certificate:

1. From Setup, enter *`Certificate and Key Management`* in the `Quick Find` box, then select **Certificate and Key Management**.
2. Click **Edit** next to the name of a Salesforce certificate.
3. Make your changes, then click **Save**.

To delete a certificate, click **Del**. If a certificate is being used as part of the configuration of your identity provider, you cannot delete it.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To create, edit, and manage certificates:

- "Customize Application"

SEE ALSO:

About Salesforce Certificates and Keys

Viewing Salesforce Certificates and Key Pairs

To view the details of a Salesforce certificate, from Setup, enter *`Certificate and Key Management`* in the `Quick Find` box, then select **Certificate and Key Management**, then click the name of a certificate.

From the certificate detail page, you can do any of the following:

- Click **Edit** to edit the label or unique name of the certificate.
- Click **Delete** to delete the certificate.
- Click **Download Certificate** to download the full Base-64 encoded certificate. This is only available for active certificates. For CA-signed certificates, you must first upload the signed certificate before you can download or use it.
- Click **Download Certificate Signing Request** for CA-signed certificates that have not yet had the signed certificate uploaded.
- Click **Upload Signed Certificate** to upload the CA-signed certificate or to upload it again.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To create, edit, and manage certificates:

- "Customize Application"

SEE ALSO:

About Salesforce Certificates and Keys

Setting Up Mutual Authentication Certificates

Identity Providers and Service Providers

An *identity provider* is a trusted provider that lets you use single sign-on to access other websites. A *service provider* is a website that hosts applications. You can enable Salesforce as an identity provider and define one or more service providers. Your users can then access other applications directly from Salesforce using single sign-on. Single sign-on can be a great help to your users: instead of having to remember many passwords, they only have to remember one. Plus, the applications can be added as tabs to your Salesforce organization, which means users don't have to switch between programs.

Before you can enable Salesforce as an identity provider, you have to set up a domain.

Enabling Salesforce as an identity provider requires a Salesforce certificate and key pair that is signed by an external certificate authority (CA-signed) or self-signed. If you haven't generated a Salesforce certificate and key pair, one is automatically created for you when you enable Salesforce as an identity provider. You also have the option of picking an already generated certificate, or creating one yourself.

Salesforce uses the SAML 2.0 standard for single sign-on 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:

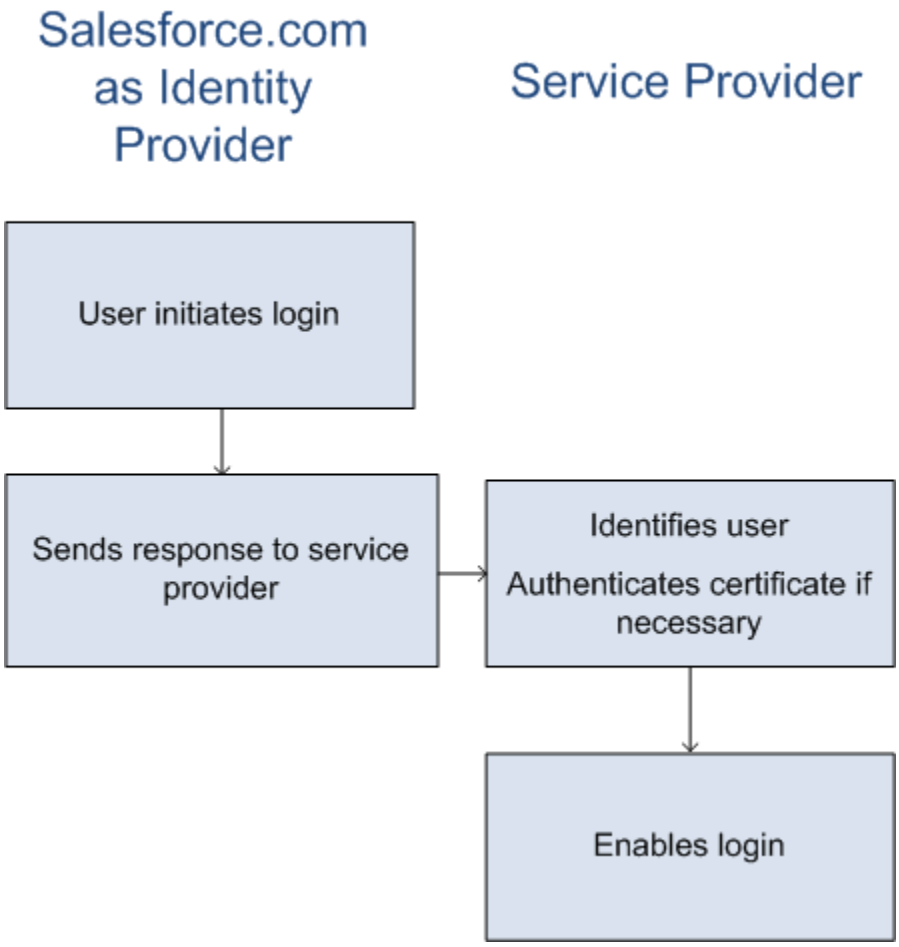
- "Customize Application"

Using Identity Providers and Service Providers

Salesforce supports the following:

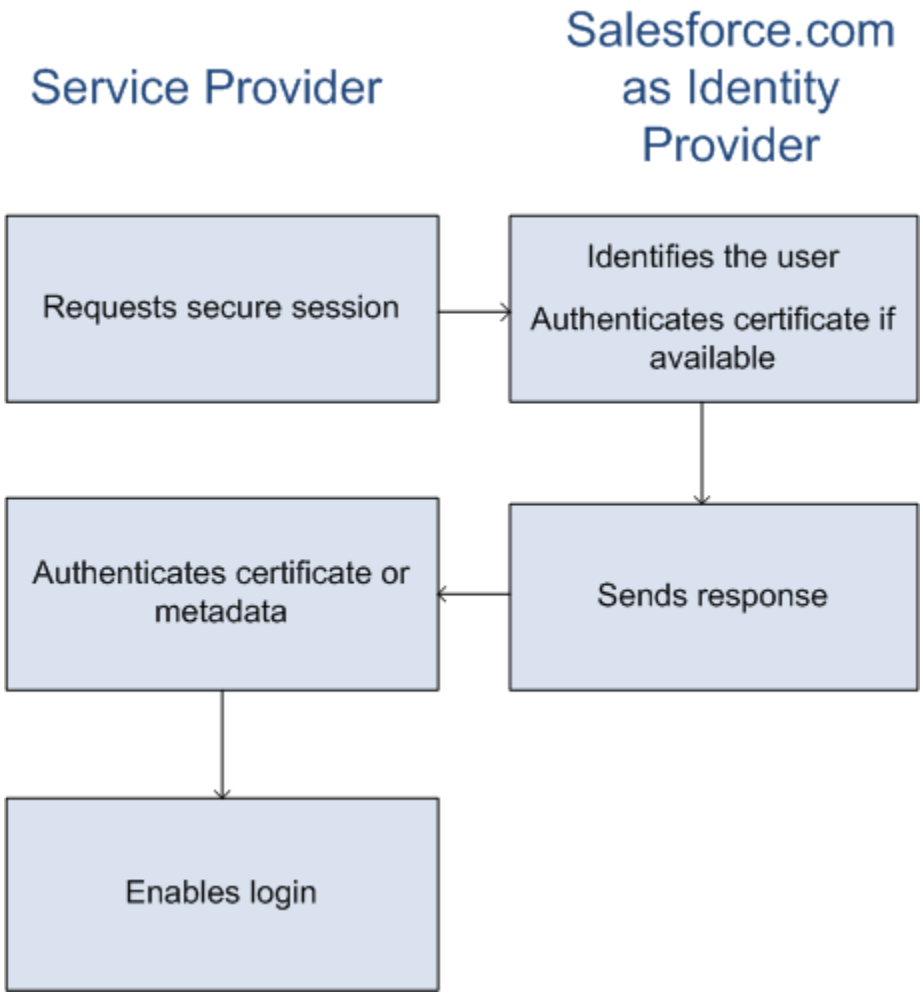
- Identity-provider-initiated login—when Salesforce logs in to a service provider at the initiation of the end user
- Service-provider-initiated login—when the service provider requests Salesforce to authenticate a user, at the initiation of the end user

The following is the general flow when Salesforce as an identity provider logs in to a service provider.



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, they are logged in to the service provider.

The following is the general flow when a service provider initiates login and uses Salesforce to identify the user.



1. The service provider sends a valid SAML request. The endpoint is automatically generated when the service provider is defined—the `SP-Initiated POST Endpoint`.
2. Salesforce identifies the user included 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 was included as part of the definition, Salesforce authenticates the certificate.

   Note: If a certificate is included in the service provider definition, and the SAML request does not contain a certificate, the request fails. The user is not logged in using Salesforce. If the definition does not include a certificate, and the request includes a signature, the request succeeds if the user is identified correctly.

3. If the user isn't already logged in to Salesforce, they are prompted to do so.

4. Salesforce sends a SAML response to the service provider.
5. The service provider authenticates the SAML response sent by Salesforce. If the user has been authenticated, they are logged in to the service provider. The user is also logged in to Salesforce.

   Important: Salesforce doesn't provide any mechanism for automatically logging the user 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:

Examples Using 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 Using Identity Providers and Service Providers

Enable Salesforce as an Identity Provider

To enable Salesforce as an identity provider:

1. Set up a domain using My Domain, and deploy it to all users.
2. From Setup, enter *Identity Provider* in the Quick Find box, then select **Identity Provider**, and then click **Enable Identity Provider**.
3. By default, a Salesforce identity provider uses a self-signed certificate generated automatically 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, following these steps.

   a. Create and import a new CA-signed certificate. For instructions, see About Salesforce Certificates and Keys .
   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 define service providers by creating connected apps (From Setup, enter *Apps* in the Quick Find box, then select **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"

SEE ALSO:

Identity Providers and Service Providers
Creating Certificates and Key Pairs

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.

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

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 into 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

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.

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"

```
<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>
```

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 Using Identity Providers and Service Providers

This section contains two examples of setting up Salesforce as an identity provider, then setting up two different service providers:

- Google Apps —shows service-provider initiated login.
- Salesforce—shows identity-provider initiated login.

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"

Setting up Single Sign-on to Google Apps Example

This example shows how to set up single sign-on from Salesforce to Google Apps. In this example, Google is the service provider, and Google Apps is the app provided by the service provider.

For this example to work:

- You must already have a Premier Edition Google Apps account
- Your Salesforce organization must be set up for single sign-on using SAML 2.0

The general steps are as follows, with more specifics on each step below.

1. Generate a domain name and enable an identity provider in your Salesforce organization.
2. Define the service provider in Salesforce.
3. Enable the Salesforce user and profile.
4. Setup Google Apps.
5. Test your implementation.

Generating a Domain Name and Enabling an Identity Provider

To prepare your Salesforce organization for this example, generate a domain name and enable Salesforce as an identity provider:

1. Log in to Salesforce.
2. Generate a domain name for your organization:

a. From Setup, enter *My Domain* in the Quick Find box, then select **My Domain**, enter a new subdomain name, and click **Check Availability**.

b. If the name is available, click the **Terms and Conditions** check box, then click **Register Domain**.

Important: You must deploy your domain name before you can enable Salesforce as an identity provider.

3. Enable Salesforce as an identity provider:

a. From Setup, enter *Identity Provider* in the Quick Find box, then select **Identity Provider**.

b. Click **Enable**.

c. Click **Download Certificate**. Remember where you save the certificate, as you will upload it later.

Defining a Service Provider

To define the service provider:

1. Log in to Salesforce.
2. From Setup, enter *Apps* in the Quick Find box, then select **Apps**.
3. Click **New** in the Connected Apps section and for Connected App Name, enter Google Apps.
4. In the Web App Settings area, select **Enable SAML** and then enter the following information:

Field	Value
ACS URL	The URL for your Google App account, such as https://www.google.com/a/respond.info
Entity ID	google.com
Subject Type	Federation ID

5. Click **Save**.
6. To authorize access to this app, enter *Connected Apps* in the Quick Find box, select the option for managing connected apps, and then click the name of the application. Then select the current user's profile.
7. Copy the value in the SP-Initiated Redirect Endpoint field. You will use this value later.

Mapping the Salesforce user to the Google Apps user

1. 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**.
2. Click **Edit**.
3. For Federation ID, enter the username you use to sign into Google Apps, for example, JSmith@TGroup.com.
4. Click **Save**.

Setting up Google Apps

1. Log in to your Google Apps account.

2. Click the **Advanced tools** tab, then the **Set up single sign-on (SSO)** link.
3. Check the `Enable Single Sign-on` checkbox.
4. For `Sign-in page URL`, enter the URL copied from the `SP-Initiated Redirect Endpoint` field, from defining a service provider.
5. For `Sign-out page URL`, specify the URL where you want your users to go after they log out of Google Apps, such as, `http://www.mydomain.salesforce.com`.
6. For `Change password URL`, use the following URL: `https://mydomain.salesforce.com/_ui/system/security/ChangePassword`, where *`mydomain`* is the name you specified for your custom domain when you generated your domain.
7. For `Verification certificate`, upload the certificate you downloaded from enabling an identity provider.
8. Click **Save Changes**.

Testing Your Implementation

To verify that your Salesforce organization can use single sign-on to Google Apps:

1. Log out of Google Apps and Salesforce.
2. Try to access a Google app page, such as `http://docs.google.com/a/respond.info/` or `http://mail.google.com/a/respond.info/`.
3. You are redirected to a Salesforce sign-on page. After you login, you are at the specified Google app page.

An alternate test is to add the Google App to a web tab in your Salesforce organization.

1. Log in to Salesforce.
2. From Setup, enter *`Tabs`* in the `Quick Find` box, then select **Tabs**, then click **New** in the `Web Tabs` section.
3. Choose a tab layout and click **Next**.
4. Enter a label to display on the tab.
5. Use the default name. This is the same as the label.
6. Click the `Tab Style` lookup icon to display the Tab Style Selector. Select an icon. Keep all other defaults.
7. Click **Next**.
8. In the Button or Link URL text box, enter a Google App page, such as `docs.google.com/a/respond.info/` or `mail.google.com/a/respond.info/`, then click **Next**.

   Note: This has to be an absolute URL, that is, it must contain either `http://` or `https://`.

9. Click **Next** and **Save**.
10. Click the new tab at the top of your page. You are automatically logged into the specified Google app page.

Setting up Single Sign-on from Salesforce to Salesforce

This example shows how to set up a Salesforce app to initiate single sign-on from one Salesforce organization to another.

The initiating Salesforce organization, that is, the organization that you want to initially log into, acts as the *identity provider*. The Salesforce organization that you want to access using an app acts as the *service provider*.For example, suppose you have two Salesforce organizations: a sales organization and an ideas organization. You can set up single sign-on between the two organizations so your users only have to log into and remember the password for one.

For this example to work, your initiating Salesforce organization must be set up for single sign-on using SAML 2.0. The general steps are as follows, with more specifics on each of these steps.

1. Generate a domain name and enable an identity provider in the Salesforce organization that is acting as an identity provider.
2. Set up the Salesforce organization that is acting as a service provider.
3. Define the service provider app in the Salesforce organization that is acting as an identity provider.
4. Test your implementation.

Generating a Domain Name and Enabling an Identity Provider

All the work in the following steps is done on the Salesforce organization that is acting as the identity provider.

To prepare your Salesforce organization for this example, generate a domain name and enable Salesforce as an identity provider:

1. Log in to Salesforce.
2. Generate a domain name for your organization:
   a. From Setup, enter *My Domain* in the Quick Find box, then select **My Domain**, enter a new subdomain name, and click **Check Availability**.
   b. If the name is available, click the **Terms and Conditions** check box, then click **Register Domain**.

      Important: You must deploy your domain name before you can enable Salesforce as an identity provider.

3. Enable Salesforce as an identity provider:
   a. From Setup, enter *Identity Provider* in the Quick Find box, then select **Identity Provider**.
   b. Click **Enable**.
   c. Click **Download Certificate**. Remember where you save the certificate, as you will upload it later.

Setting up a Salesforce Organization as Service Provider

To configure a second Salesforce organization as the service provider:

1. Log in to the Salesforce organization that acts as the service provider.
2. Enable and configure SAML:
   a. From Setup, enter *Single Sign-On Settings* in the Quick Find box, then select **Single Sign-On Settings**, then click **Edit**.
   b. Select the SAML Enabled check box.
   c. Use the following settings:

Field	Value
SAML Version	2.0
Issuer	The identity provider issuer URL, created when the identity provider is set up. For example, https://mycustomdomain.salesforce.com.
Identity Provider Certificate	Browse for the certificate you downloaded in enabling an identity provider.

Field	Value
SAML User ID Type	Select Assertion contains the Federation ID from the User object
SAML User ID Location	Select User ID is in the NameIdentifier element of the Subject statement

d. Click **Save**.

e. Copy and save the values from the fields Salesforce Login URL and Entity ID. You need these values later, when defining the Salesforce service provider.

3. Link your user in the service provider organization to the user in the identity provider organization:

a. From your personal settings, enter *Advanced User Detail* in the Quick Find box, then select **Advanced User Detail**. No results? Enter *Personal Information* in the Quick Find box, then select **Personal Information**.

b. Click **Edit**.

c. For Federation ID, enter the username used to sign into theSalesforce identity provider organization, for example, IDP_org@TGroup.com.

d. Click **Save**.

Defining the Service Provider in the Identity Provider Organization

To define the service provider, you create a SAML enabled Web App as a connected app:

1. Log in to the Salesforce organization that acts as the identity provider.
2. From Setup, enter *Apps* in the Quick Find box, then select **Apps**, then in the Connected Apps section, click **New**.
3. Specify the following information:

Field	Value
Connected App Name	Salesforce Service Provider
Contact Email	Contact Salesforce should use for contacting you or your support team.
Enable SAML	Select this option to enter service provider details.
Entity Id	Use the Entity ID from setting up the service provider
ACS URL	Use the Salesforce Login URL from setting up the service provider
Subject Type	Select Username

4. Click **Save**.
5. Select the profiles allowed to access this service provider. You must select the current user's profile for this example to work.
6. Click **Save**.
7. Copy down the value of the IdP-Initiated Login URL field. You will use this value later, in testing.

Testing Your Implementation

To verify that your Salesforce organizations can use single sign-on to connect, create a web tab:

1. Log in to the Salesforce organization that is acting like a service provider.
2. From Setup, enter *Tabs* in the Quick Find box, then select **Tabs**, then click **New** in the Web Tabs section.
3. Choose a tab layout and click **Next**.
4. Enter a label to display on the tab.
5. Use the default name. This is the same as the label.
6. Click the Tab Style lookup icon to display the Tab Style Selector. Select an icon.
7. Click **Next**.
8. In the Button or Link URL text box, enter the value of the IdP-Initiated Login URL field from defining the service provider, then click **Next**.

   Note: This has to be an absolute URL, that is, it must contain either http:// or https://.

9. Click **Next**, then **Save**.
10. Click the new tab at the top of your page. If you have logged out of the Salesforce organization that acts as the identity provider, you are prompted to log in. Once you are logged in, you should see the Salesforce organization that acts as the identity provider in the tab.

SEE ALSO:

Identity Providers and Service Providers

Configuring Remote 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 will fail.

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.

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:

- "Modify All Data"

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.

Named Credentials

A named credential specifies the URL of a callout endpoint and its required authentication parameters in one definition. You can simplify the setup of authenticated callouts by specifying a named credential as the callout endpoint. You can instead specify a URL as the callout endpoint and register that URL in your organization's remote site settings. However, in that case, you handle the authentication yourself, for example, in your code for an Apex callout. Doing so can be less secure and is especially complicated for OAuth authentication.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in all editions

Salesforce manages all authentication for callouts that specify a named credential as the callout endpoint so that you don't have to. You can also skip remote site settings, which are otherwise required for callouts to external sites.

Named credentials are supported in these types of callout definitions:

- Apex callouts
- External data sources of these types:
  - Lightning Connect: OData 2.0
  - Lightning Connect: OData 4.0
  - Lightning 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 organizations, 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.

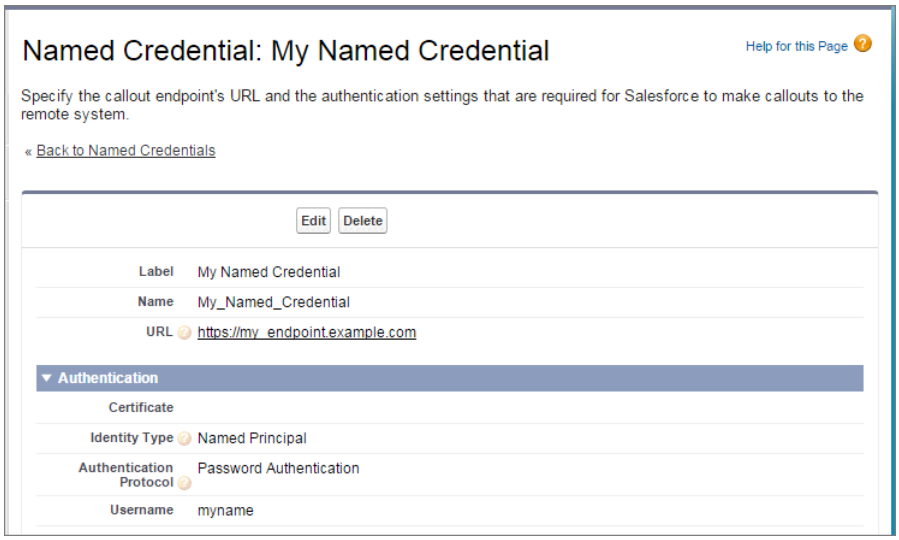
Named credentials support basic password authentication and OAuth 2.0. You can set up each named credential to use an organization-wide named principal or to use per-user authentication so that users can manage their own credentials.

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*.

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.



You can code the callout endpoint as the URL instead of the named credential, but your code then handles the authentication. Our example uses basic password authentication, but keep in mind that OAuth authentication is much 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.

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

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.

Named credentials are supported in these types of callout definitions:

- Apex callouts
- External data sources of these types:
  - Lightning Connect: OData 2.0
  - Lightning Connect: OData 4.0
  - Lightning 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, create, edit, or delete named credentials:

- "Modify All Data"

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.

Field	Description

`URL`	The URL or root URL of the callout endpoint. Must begin with *`http://`* or *`https://`*.
	You can append a specific path when you reference the named credential from the callout definition. For example, an Apex callout could reference the named credential as follows.
	`HttpRequest req = new HttpRequest();`
	`req.setEndpoint('callout:My_Named_Credential/some_path');`

`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 organization. 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 About External Authentication Providers on page 623.
`Scope`	Specifies the scope of permissions to request for the access token. Your authentication provider determines the allowed values. See Using the Scope Parameter on page 653. 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.

Field	Description
`Start Authentication Flow on Save`	To authenticate to the external system and obtain an OAuth token, select this checkbox. This authentication process is called an OAuth flow. When you click **Save**, the external system prompts you to log in. After successful login, the external system grants you an OAuth token for accessing its data from this org. Redo the OAuth flow when you need a new token—for example, if the token expires—or if you edit the `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`*.

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**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

Available in all editions

USER PERMISSIONS

To edit permission sets and user profiles:
- "Manage Profiles and Permission Sets"

SEE ALSO:

Define a Named Credential

Named Credentials

About Identity Connect

Identity Connect provides Active Directory integration.

Identity Connect provides Active Directory integration with Salesforce via a service which runs on either Windows or Linux platforms. This integration includes syncing Active Directory users with either Salesforce or Identity Connect acting as the Identity Service Provider (IDP) for Single Sign On (SSO) Active Directory integration when logging into Salesforce.

IN THIS SECTION:

Installing Identity Connect

Enabling Identity Connect

SEE ALSO:

Salesforce Identity Connect Implementation Guide

Installing Identity Connect

Enabling Identity Connect

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.

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.

SEE ALSO:

About Identity Connect

Enabling Identity Connect

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"

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.

Walk Through It: create, edit, and assign a permission set

SEE ALSO:

Salesforce Identity Connect Implementation Guide

About Identity Connect

Installing Identity Connect

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"

Monitor Your Organization

About the System Overview Page

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.

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). 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
- Portal roles

Note: The object limit percentages are truncated, not rounded. For example, if your organization uses 95.55% of the limit for a particular customization, the object limit displays 95%.

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"

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 organization in a 24 hour period; limits are not on a per-user basis. When an organization exceeds a limit, all users in the organization may be temporarily blocked from making additional calls. Calls will be 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 portal roles for an organization is 5000. This limit includes portal 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 for each of your portals and communities. Additionally, delete any unused portal roles. If you still require more portal roles, please contact Salesforce Customer Support.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

Monitor Storage Resources

See 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 and data storage. File storage includes files in attachments, the Documents tab, the Files tab, the File field, Salesforce CRM Content, Chatter files (including user photos), 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
- Notes
- Opportunities
- Opportunity Splits
- Orders
- Quotes
- Quote Template Rich Text Data

- Solutions
- Tags: Unique tags
- Tasks

Storage Capacity

For file storage, Contact Manager, Group, Professional, Enterprise, Performance, and Unlimited Editions are allocated a per-user limit multiplied by the number of users in the organization plus an additional per-organization allocation. For example, a Professional Edition organization with 10 users receives 11 GB of file storage, or 100 MB per user multiplied by 10 users plus an additional 10 GB. A Professional Edition organization with 100 users receives 20 GB of file storage, or 100 MB per user multiplied by 100 users plus an additional 10 GB.

For data storage, Contact Manager, Group, Professional, Enterprise, Performance, and Unlimited Editions are allocated either 1 GB or a per-user limit, whichever is greater. For example, a Professional Edition organization 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 organization with 100 users receives more than the 1 GB minimum because 100 users multiplied by 20 MB per user is 2,000 MB.

The values in the Storage Allocation Per User License column below apply to Salesforce and Salesforce Platform user licenses.

Salesforce Edition	Data Storage Minimum Per Organization	Data Storage Allocation Per User License	File Storage Allocation Per Organization	File Storage Allocation Per User License
Contact Manager	1 GB	20 MB	11 GB	612 MB
Group	1 GB	20 MB	11 GB	612 MB
Professional	1 GB	20 MB	11 GB	612 MB
Enterprise	1 GB	20 MB	11 GB	2 GB
Performance	1 GB	120 MB	11 GB	2 GB
Unlimited	1 GB	120 MB	11 GB	2 GB
Developer	5 MB	N/A	20 MB	N/A
Personal	20 MB (approximately 10,000 records)	N/A	20 MB	N/A

If your organization uses custom user licenses, contact Salesforce to determine if these licenses provide additional storage. For a description of user licenses, see User Licenses Overview.

Viewing Storage Usage

To view your organization'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 organization's storage usage isn't updated immediately, if you import or add a large number of 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 additional 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

Administrators can monitor all login attempts for their organization 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

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 of user logins to your Salesforce organization 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 to your Salesforce organization for the past six months. This report includes logins through the API.
   - **gzipped Excel csv file**: Download a CSV file of all user logins to your Salesforce organization for the past six months. This report includes logins through the API. The file is compressed, which is the preferred option for quickest download time.
3. Select the file contents. All Logins 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 new 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 drop-down 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) may 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, click **Download...**.

Note: For security purposes, Salesforce may require users to pass a CAPTCHA user verification test to export data from their organization. This simple text-entry test prevents malicious programs from accessing your organization's data. To pass the test, users must correctly type the two words displayed on the overlay into the overlay's text box field. Note that the words entered into the text box field 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.

SEE ALSO:

Identity Verification History

Identity Verification History

As an administrator, use the Identity Verification History to monitor and audit the past six months of your org users' identity verification attempts. 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.

EDITIONS

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

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. • 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. • 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. • One-time password—An authenticator app generated a time-based, one-time password (TOTP) on the user's mobile device. • Salesforce Authenticator—Salesforce Authenticator sent a notification to the user's mobile device to verify account activity. • Text message—Salesforce sent a text message with a verification code to the user's mobile device.
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.

Field	Description
	• 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 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) may 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) may 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.

Field	Description
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. • 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

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.

Metrics
In the context of login forensics, metrics are roll-up aggregations of login events over time. Use metrics to determine atypical behavior within your organization.

Administrators can track events using two API objects: LoginEvent and PlatformEventMetrics. There's no user interface for login forensics. Use the Force.com IDE, Workbench, or other development tools to interact with this feature.

Note: Login forensics isn't available on government pods.

Considerations for Using Login Forensics

Before you get started with Login Forensics, keep in mind some considerations for use.

- This feature is API only. You can't view events or metrics in the user interface.
- Login events are retained for 14 days by default.
- Metrics are retained for 90 days by default.
- Because login forensics uses an asynchronous queuing technology similiar to `@future` calls in Apex, login data might be delayed when querying.

EDITIONS

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

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"

Metrics in Login Forensics

Forensic investigations often begin with a roll-up of login events, and metrics are roll-up aggregations of login events over time.

Login forensics can be:

- A count.
- A count followed by an aggregation.

Each time-series metric contains:

- A query that uses aggregate functions.
- An hourly sampling interval.
- A frequency time frame, such as from 01-01-2015 12:00 to 01-01-2015 1:00.

EDITIONS

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

With this information, you can find anomalies by viewing summary data and then following up with more detailed queries to perform additional investigations. All metrics are generated once per hour and are accessed using the PlatformEventMetrics object.

In the following example, the total number of logins is four, but the aggregated number of logins by each user differs. The user with an ID that ends in "122" logged in once, and another user logged in three times.

Login Time	User Id
12:00	005000000000122
12:15	005000000000123
12:31	005000000000123
12:47	005000000000123

This table shows the collected metrics for the 12:00-1:00 time frame.

Metric Type	Aggregation Field Name	Aggregation Field Value	Value
`NumLogins`	`Null`	`Null`	4
`NumLoginsByUser`	`UserId`	005000000000122	1
`NumLoginsByUser`	`UserId`	005000000000123	3

Monitoring Training History

As an administrator, it is important 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**, **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Database.com** Editions

USER PERMISSIONS

To view training history:
- "Manage Users"

Monitor Setup Changes

The setup audit trail history helps you track the recent setup changes that you and other administrators have made to your organization. Audit history can be especially useful in organizations with multiple administrators.

To view the setup audit trail history, from Setup, enter *View Setup Audit Trail* in the Quick Find box, then select **View Setup Audit Trail**. To download your organization's full setup history for the past 180 days, click the **Download** link.

The setup audit trail history shows you the 20 most recent setup changes made to your organization. It lists the date of the change, who made it, and what the change was. Additionally, if a delegate (such as an administrator 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 administrator and the administrator makes a setup change, the administrator's username is listed.

The setup audit trail history tracks the following types of changes:

Setup	Changes Tracked
Administration	• Company information, default settings such as language or locale, and company message changes • Multiple currency setup changes • User, portal user, role, permission set, and profile changes • Email address changes for any user • Deleting email attachments sent as links • Creating, editing, or deleting email footers • Record type changes, including creating or renaming record types and assigning record types to profiles • Changes to divisions, including creating and editing divisions, transferring divisions, and changing users' default division • Adding or deleting certificates • Domain name changes • Enabling or disabling Salesforce as an identity provider
Customization	• Changes to user interface settings, such as collapsible sections, Quick Create, hover details, or the related list hover links • Page layout, action layout, and search layout changes • Changes to compact layouts • Changes to the Salesforce1 navigation menu • Changes made using inline editing • Custom field and field-level security changes, including changes to formulas, picklist values, and custom field attributes, like the format of auto-number fields, manageability, or masking of encrypted fields • Changes to lead settings, lead assignment rules, and lead queues • Changes to activity settings

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 view audit trail history:
- "View Setup and Configuration"

Setup	Changes Tracked
	• Changes to support settings, business hours, case assignment and escalation rules, and case queues • Any changes made by Salesforce Customer Support at your request • Changes to tab names, including tabs that you reset to the original tab name • Changes to custom apps (including Salesforce console apps), custom objects, and custom tabs • Changes to contract settings • Changes to forecast settings • Enabling or disabling Email-to-Case or On-Demand Email-to-Case • Changes to custom buttons, links, and s-controls, including standard button overrides • Enabling or disabling drag-and-drop scheduling • Enabling, disabling, or customizing similar opportunities • Enabling or disabling quotes • Changes to data category groups, data categories, and category-group assignments to objects • Changes to article types • Changes to category groups and categories • Changes to Salesforce Knowledge settings • Changes to ideas settings • Changes to answers settings • Changes to field tracking in feeds • Changes to campaign influence settings • Activating or deactivating critical updates • Enabling or disabling Chatter email notifications • Enabling or disabling Chatter new user creation settings for invitations and email domains • Changes to validation rules
Security and Sharing	• Public groups, sharing rule changes, and organization-wide sharing, including the **Grant Access Using Hierarchies** option • Password policy changes • Password resets • Session settings changes, such as changing the session timeout setting • Changes to delegated administration groups and the items delegated administrators can manage. Setup changes made by delegated administrators are tracked as well. • How many records a user emptied from their Recycle Bin and from the organization's Recycle Bin • Changes to SAML (Security Assertion Markup Language) configuration settings • Changes to Salesforce certificates • Enabling or disabling identity providers • Changes to named credentials • Changes to service providers • Changes to Platform Encryption setup.

Setup	Changes Tracked
Data Management	• Mass delete use, including when a mass delete exceeds the user's Recycle Bin limit of 5000 deleted records. The oldest, excess records are permanently removed from the Recycle Bin within two hours of the mass delete transaction time. • Data export requests • Use of the campaign member import wizard • Mass transfer use • Changes to reporting snapshots, including defining, deleting, or changing the source report or target object on a reporting snapshot • Import wizard use
Development	• Changes to Apex classes and triggers • Changes to Visualforce pages, custom components, or static resources • Changes to Lightning Pages • Changes to action link templates • Changes to custom settings • Changes to custom metadata types and records • Changes to remote access definitions • Changes to Force.com Sites settings
Various Setup	• Creation of an API usage metering notification • Changes to territories • Changes to process automation settings • Changes to approval processes • Creation and deletion of workflow actions • Changes to Visual Workflow files • Packages from Force.com AppExchange that you installed or uninstalled
Using the application	• Changes to account team and opportunity team selling settings • Activation of Google Apps services • Changes to mobile configuration settings, including data sets, mobile views, and excluded fields • A user with the "Manage External Users" permission logging into the partner portal as a partner user • A user with the "Edit Self-Service Users" permission logging into the Salesforce Customer Portal as a Customer Portal user • Enabling or disabling a partner portal account • Disabling a Salesforce Customer Portal account • Enabling or disabling a Salesforce Customer Portal and creating multiple Customer Portals • Creating and changing entitlement processes and entitlement templates • Enabling or disabling self-registration for a Salesforce Customer Portal

Setup	Changes Tracked
	• Enabling or disabling Customer Portal or partner portal users

SEE ALSO:

Security Health Check

Track Field History

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 history of the following standard objects.

- Accounts
- Assets
- Cases
- Contacts
- Entitlements
- Service contracts
- Contract line items
- Contracts
- Leads
- Opportunities
- Articles
- Solutions
- Products

EDITIONS

Available in: Salesforce Classic

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

Standard Objects are not available in **Database.com**

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 prior to 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 retained for a maximum of 18 months.

Considerations

- 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.

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

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**.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

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"

Salesforce tracks history from this date and time forward. Changes made prior to this date and time are not included.

SEE ALSO:

Track Field History

Track Field History for Custom Objects

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:

Track Field History

EDITIONS

Available in: Salesforce Classic

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

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:

Track Field History

EDITIONS

Available in: Salesforce Classic

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 ten 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` object for your related history lists, such as Account History, to specify Field Audit Trail retention policies for the objects that you want to archive. You can then deploy the object by using the Metadata API (Workbench or Force Migration Tool). In production organizations that have Field Audit Trail enabled, data is archived by default after 18 months. In sandbox organizations, the default is one month. You can update the retention policies as often as you like.

You can set Field Audit Trail policies on the following objects.

- Accounts
- Cases
- Contacts
- Leads
- Opportunities
- Assets
- Entitlements
- Service Contracts

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To specify a field history retention policy:
- "Retain Field History"

- Contract Line Items
- Solutions
- Products
- Price Books
- Custom objects with field history tracking enabled

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: For some time after the initial GA release, data might not be automatically deleted from the History related list and may reside in both the `FieldHistoryArchive` object and in the History related list. Salesforce reserves the right to delete archived data from the History related list in accordance with the customer-defined policy in future releases.

Note: If your organization has Field Audit Trail enabled, previously archived data isn't encrypted if you subsequently turn on Platform Encryption. 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 are encrypted as they are created, and 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 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.

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 a 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 0 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.

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

When you've set your trace flags, monitor logging for users, Apex classes, and Apex triggers in the Developer Console or in Setup.

You can retain and manage the debug logs for specific users, including yourself, and for classes and triggers.

To view saved debug logs, from Setup, enter *Debug Logs* in the Quick Find box, then select **Debug Logs**. When you've started retaining debug logs, you can view, download, or delete your logs from this page.

SEE ALSO:

Set Up Debug Logging

Viewing Debug Logs

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"

Set Up Debug Logging

To activate debug logs for users, Apex classes, and Apex triggers, configure trace flags and debug levels in the Developer Console or in Setup.

You can retain and manage the debug logs for specific users, including yourself, and for classes and triggers.

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.
- Each organization can retain up to 50 MB of debug logs. Once your organization has reached 50 MB of debug logs, the oldest debug logs start being overwritten.

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"

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.

Configure Trace Flags in Setup

To configure trace flags and debug levels from Setup, complete these actions.

1. Navigate to the appropriate Setup page.
   - For user-based trace flags and debug levels, enter *Debug Logs* in the Quick Find box, then click **Debug Logs**.
   - For class-based trace flags and debug levels, 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 and debug levels, 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, complete these actions.
   - To add a trace flag, click **New**.
   - To change an existing trace flag, click an option in the Action column.
     - To delete a trace flag, click **Remove**.
     - To modify a trace flag, click **Edit**.
     - To modify a trace flag's debug level, click **Filters**.
     - To create a debug level, click **Edit**, click the magnifying glass icon next to the Debug Level field, and then click **New**.

SEE ALSO:

Monitor Debug Logs

Viewing Debug Logs

USER PERMISSIONS	
To use the Developer Console:	"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

To view the details of a debug log, from Setup, enter *Debug Logs* in the Quick Find box, select **Debug Logs**, and then click **View** next to the debug log that you want to examine. Click **Download** to download the log as an XML file.

The debug log contains information about the transaction, such as if it was successful, the size of the log (in bytes), how long the transaction took in milliseconds, and so on. The log itself contains additional information about the transaction, depending on the filters set for the user.

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

Configure Salesforce Mobile Apps

Salesforce1

Salesforce1 Mobile App Setup Options

See the many options for customizing the Salesforce1 mobile app, to make it an effective on-the-go tool for your users' business needs.

All Salesforce1 customization options are available from the Setup menu, which you access from the upper-right corner of any Salesforce page. For your convenience, you can access many Salesforce1 settings pages more quickly from the Salesforce1 Quick Start setup page. In Salesforce Classic, from Setup, click **Salesforce1 Quick Start** (near the top of the Setup menu). In Lightning Experience, from Setup, enter *Salesforce1 Quick Start* in the Quick Find box, then select **Salesforce1 Quick Start**.

Note: We recommend using Google Chrome for the Salesforce1 Quick Start setup page. Microsoft Internet Explorer 9 or later and Mozilla Firefox are also supported.

EDITIONS

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

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

Here are the Salesforce1 customization options you can consider for your organization.

- Do some basic setup using the Salesforce1 Wizard. From the Salesforce1 Quick Start page, click **Launch Quick Start Wizard**.
- Define the users who can access Salesforce1.
  - For the downloadable apps, from the Salesforce1 Quick Start page, click **App Security Controls**.
  - For the mobile browser app, from the Salesforce1 Quick Start page, click **Mobile Browser Option**.
- Customize how data appears in Salesforce1. 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 in Salesforce1. From the appropriate object management settings, go to Page Layouts.
  - Make sure that Visualforce pages are enabled for use in Salesforce1, 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 Salesforce1 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 Salesforce1 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 Salesforce1 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 Salesforce1 and Lightning Experience Actions section of the global publisher layout so that they appear in Salesforce1. 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 Salesforce1 and Lightning Experience Actions section on the appropriate object page layout.

- Customize the options that are available in the Salesforce1 navigation menu, and the order in which items appear. From the Salesforce1 Quick Start page, click **Navigation Menu**.
- Help keep Salesforce1 users aware of important Salesforce activities by enabling in-app and push notifications. From the Salesforce1 Quick Start page, click **Notification Options**.
- Integrate third-party apps into the Salesforce1 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 Salesforce1 to match the look and feel of your company's branding. From the Salesforce1 Quick Start page, click **Salesforce1 Branding**.
- Allow the Salesforce1 downloadable apps 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 Salesforce1 Quick Start page, click **Offline Cache**.

You can also check out the *Salesforce1 Mobile App Admin Guide*, which walks you through using the Salesforce1 declarative tools in Setup to get your organization ready for the Salesforce1 mobile experience.

SEE ALSO:

Set Up the Salesforce1 Mobile App with the Salesforce1 Wizard

Set Up the Salesforce1 Mobile App with the Salesforce1 Wizard

The Salesforce1 Wizard provides an easy way to complete the essential setup tasks for Salesforce1. After you've set up Salesforce1 with this wizard, your sales reps can use Salesforce1 to run their business from their mobile devices.

Note: We recommend using Google Chrome for the Salesforce1 Wizard and the Salesforce1 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 Salesforce1 tile in the quick access carousel.

If you're using Salesforce Classic:

1. From Setup, click **Salesforce1 Quick Start**.
2. On the Salesforce1 Setup page, click **Launch Quick Start Wizard**.

Note: Although the Salesforce1 Wizard gets you up and running with basic setup tasks, it doesn't include all Salesforce1 setup tasks. For example, although you can rearrange global quick actions via the wizard, the Salesforce1 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.

EDITIONS

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 Salesforce1 wizard:

- "Customize Application"

After you've finished the wizard, you'll be directed to the Salesforce1 Quick Start setup page, which provides easy access to Salesforce1 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.

SEE ALSO:

Salesforce1 Mobile App Setup Options

Control Access to the Salesforce1 Mobile App

You can control your organization's access to the Salesforce1 downloadable apps and the Salesforce1 mobile browser app.

Based on your organization's configuration, you can:

- Enable or disable access to the Salesforce1 mobile browser app. From Setup, enter *Salesforce1 Settings* in the Quick Find box, then select **Salesforce1 Settings**. See Enable the Salesforce1 Mobile Browser App.
- Control who can access the Salesforce1 downloadable apps, 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 the Salesforce1 Downloadable Apps.

EDITIONS

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 the Salesforce1 Downloadable Apps

The Salesforce1 downloadable apps 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 the Salesforce1 downloadable apps.

You can control security and access policies for each of the Salesforce1 downloadable apps, using settings components that are installed from the managed Salesforce1 connected apps package. These components need to be installed in Salesforce:

- Salesforce1 for Android
- Salesforce1 for iOS

These components are automatically installed when one of your users installs a Salesforce1 downloadable app 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 Salesforce1 and Chatter Apps connected apps package so you can review and modify the default security and access settings before rolling out the Salesforce1 downloadable apps to your users.

When the Salesforce1 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 Salesforce1 downloadable app.

Push notifications for the Salesforce1 downloadable apps aren't managed from the Connected Apps page. To manage these settings, from Setup, enter *Notifications* in the Quick Find box, then select **Salesforce1 Notifications**.

Offline access is enabled by default when one of the Salesforce1 downloadable apps is installed. To manage these settings, from Setup, enter *Offline* in the Quick Find box, then select **Salesforce1 Offline**.

EDITIONS

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 Salesforce1 downloadable app settings:
- "Customize Application"

To view your Salesforce1 downloadable app settings:
- "View Setup and Configuration"

SEE ALSO:

Enable Salesforce1 Mobile App Notifications

Enable the Salesforce1 Mobile Browser App

You can control whether users can access the Salesforce1 mobile browser app when they log in to Salesforce from a mobile browser. By default, the mobile browser app 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 the Salesforce1 mobile browser app for your organization, and individual users can turn off the mobile browser app 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 *Salesforce1 Settings* in the Quick Find box, then select **Salesforce1 Settings**.
2. Select Enable the Salesforce1 mobile browser app 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 Salesforce1 interface. Logging in from an unsupported mobile browser loads the Salesforce Classic full site, even when this option is selected.

EDITIONS

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 Salesforce1 mobile browser app settings:

- "View Setup and Configuration"

To modify Salesforce1 mobile browser app settings:

- "Customize Application"

  "Modify All Data"

Salesforce1 Mobile App Navigation Menu

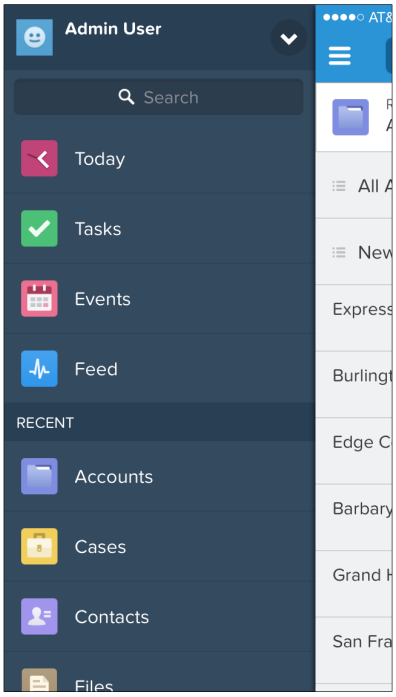
Learn about the items that can appear in the Salesforce1 navigation menu. You can customize most aspects of the navigation menu for your organization.

The icon in the Salesforce1 header opens the navigation menu.

EDITIONS

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 `Mobile Navigation` in the `Quick Find` box, then select **Salesforce1 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 Salesforce1. Available in the Salesforce1 downloadable app for iOS and the Salesforce1 mobile browser app.
Canvas apps	Appears for organizations that have enabled a canvas app to appear in the Salesforce1 navigation menu.
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 that are owned by the user, that the user created for him- or herself, and that the user or a user's groups are invited to.
Feed	Appears for organizations that have Chatter enabled.
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 Salesforce1 navigation menu.
Lightning Pages	Custom Salesforce1 app pages.

Menu Item	Description
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 from within Salesforce1. Available in the Salesforce1 mobile browser app 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 when using the Salesforce1 downloadable app for Android or the Salesforce1 mobile browser app. But the only way to include access to reports in the Salesforce1 downloadable app for iOS is to add the Reports item directly to the navigation menu.
Smart Search Items	Adds Salesforce objects to the Recent section in the menu. This item also adds a set of recently-searched 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 in Salesforce1. If you don't include this item in the navigation menu, users can't access any objects in Salesforce1. Note: If your users don't yet have a history of recent objects, they initially see a set of default objects in the Recent section. It can take up to 15 days for the objects that users work with regularly in both Salesforce1 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.
Tasks	Lists of a user's open and closed tasks and tasks that have been delegated.
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 Salesforce1 downloadable apps only.
Visualforce page tabs	Only Visualforce pages with the `Available for Salesforce mobile apps` checkbox selected will display in Salesforce1.

Things to Keep in Mind

- You can't set different menu configurations for different types of users.
- Anything that is represented by a tab in Salesforce—such as standard and custom objects, Visualforce pages, the Feed, People, or Groups—is visible for a user in the Salesforce1 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 Salesforce1, 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 Salesforce1 Navigation Menu

Notes About the Salesforce1 Navigation Menu

Enable Visualforce Pages for the Salesforce1 Mobile App

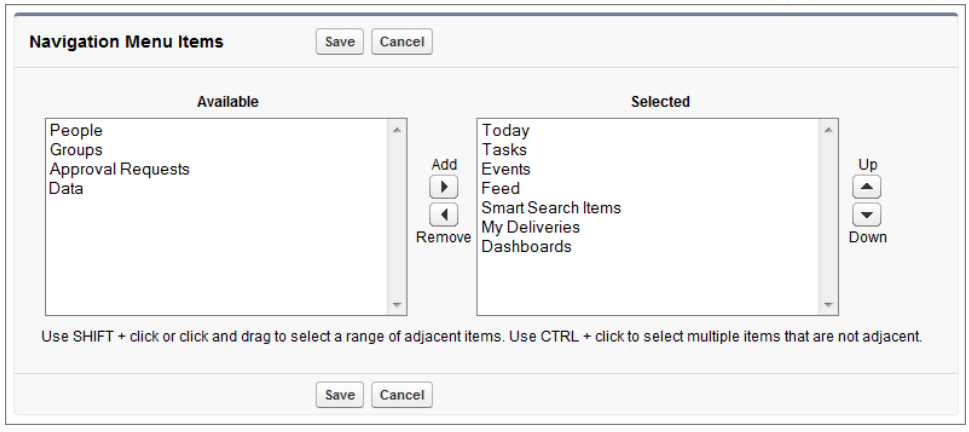
Customize the Salesforce1 Navigation Menu

Customize your users' mobile Salesforce experience by selecting the menu items, apps, Visualforce pages, or Lightning Pages to display in the Salesforce1 navigation menu.

Note: Before you can include Visualforce pages, Lightning Pages, or Lightning components in the Salesforce1 navigation menu, create tabs for them. From Setup, enter *Tabs* in the Quick Find box, then select **Tabs**.

Walk Through It: Customize the Salesforce1 Navigation Menu

1. From Setup, enter *Mobile Navigation* in the Quick Find box, then select **Salesforce1 Navigation**
2. Select items in the Available list and click **Add**.



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' Salesforce1 landing page.

4. Click **Save**.

EDITIONS

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 Salesforce1 navigation menu:

- "Customize Application"

Once saved, the navigation menu items and their order should be reflected in Salesforce1. 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 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:

Salesforce1 Mobile App Navigation Menu

Notes About the Salesforce1 Navigation Menu

Enable Visualforce Pages for the Salesforce1 Mobile App

Notes About the Salesforce1 Navigation Menu

Some objects are excluded from the Recent section in the Salesforce1 navigation menu, even if you accessed them recently.

- Tasks and events
- People, groups, notes, dashboards, and reports, if these items were added directly to the navigation menu

  Note: For the Salesforce1 downloadable app for iOS only, the Reports item is never available in the Recent section.
- List views, which are shown only on object home pages, not in the navigation menu
- Objects that aren't available in Salesforce1, including any objects that don't have a tab in the full Salesforce site

EDITIONS

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

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

About the Dashboards, Reports, Notes, Groups, and People Menu Items

If you opt to add the Dashboards, Reports, Notes, Groups, or People items to the Selected list for the Salesforce1 navigation menu, these items appear in the order you specify, just like Tasks, 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. (For Reports only, this is true when using the Salesforce1 downloadable app for Android or the Salesforce1 mobile browser app. But the only way to include access to reports in the Salesforce1 downloadable app for iOS is to add the Reports item directly to the navigation menu.

Pin an Object into the Recent Section

Users can customize the objects that appear in the Recent section of the Salesforce1 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.

SEE ALSO:

Salesforce1 Mobile App Navigation Menu

Customize the Salesforce1 Navigation Menu

Salesforce1 Mobile App Notifications

EDITIONS

Salesforce1 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.

Two types of notifications can appear to Salesforce1 users.

- *In-app notifications* keep users aware of relevant activity while they're using Salesforce1. 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 Salesforce1 downloadable app 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.

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.

Terms and Conditions for Including Full Content in Push Notifications

If you go to the Notifications Settings page on the full site and select the option to include full content in push notifications, a pop-up window displays several terms and conditions. If you click **OK** in the pop-up window, you're agreeing to these terms and conditions on behalf of your company.

Salesforce1 Mobile Push Notifications

The Salesforce1 full-content push notifications feature will provide your organization's Users (collectively, "you" or "your") with real-time updates — for example, whenever you receive an approval request or a mention in a post. The frequency of notifications sent to you will depend on the number of these actions occurring for you.

Enable or disable full-content push notifications at any time from Setup by entering `Notifications Settings` in the `Quick Find` box, selecting **Notifications Settings**, and then selecting or deselecting "Include full content in push notifications."

For Users within your organization whose mobile devices run the iOS platform, usage of the full-content push notifications feature will result in transmission of your data contained in those notifications (potentially including Customer Data and/or Confidential Information, as those terms are defined in the subscription agreement that governs your use of Salesforce products) to Apple Inc. and its affiliated entities (collectively, "Apple"). To the extent that any such data is transmitted to Apple, Salesforce is not responsible for the privacy, security, or integrity of that data.

If you are authorized by the company that has purchased the subscriptions associated with your use of the Salesforce Services to enable this functionality and agree to these terms and conditions, please confirm your acceptance by checking the box marked "OK" below. If you are not authorized by such company to accept these terms and enable this functionality, you must click "Cancel".

SEE ALSO:

Enable Salesforce1 Mobile App Notifications

Enable Salesforce1 Mobile 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 *Salesforce1 Notifications* in the Quick Find box, then select **Salesforce1 Notifications**.
2. Select the notifications you want your Salesforce1 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 checked the box to include full content in push notifications, a pop-up appears displaying terms and conditions. Click **OK** or **Cancel**.

   By enabling this option, you're agreeing to the terms and conditions on behalf of your company. For details, see Salesforce1 Mobile App Notifications on page 724.

A user can receive approval requests in Salesforce1 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.

EDITIONS

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"

SEE ALSO:

Salesforce1 Mobile App Notifications

Salesforce1 Mobile App Offline Access

Salesforce1 can cache recently accessed data so it's available when a user's device is offline or unable to connect to Salesforce. Offline access is currently read-only, and is available in the Salesforce1 downloadable apps for iOS and Android devices.

Offline access is enabled the first time a user in your organization installs one of the Salesforce1 downloadable apps. You can manage this setting on the Salesforce1 Offline page in Setup.

With offline access turned on, the app automatically caches a user's most recently accessed records for the objects listed in the Recent section of the Salesforce1 navigation menu, and a user's recent dashboards. Recently accessed records are determined by a user's activities in both the mobile app and the full Salesforce site. In addition, the app caches much of the data that a user accesses during a Salesforce1 session.

Cached data is encrypted and stored in a secure, persistent data store.

This table lists the data and Salesforce1 elements that are available offline.

EDITIONS

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

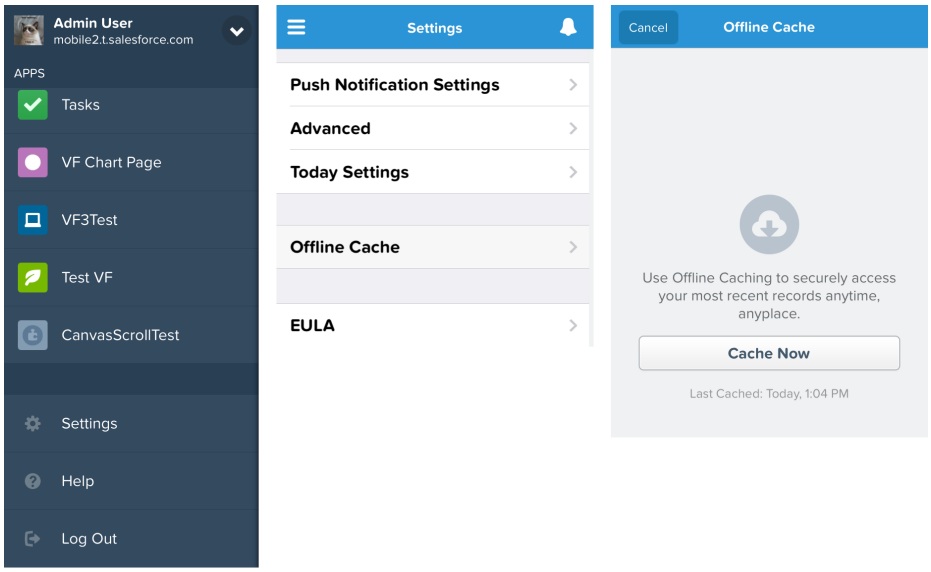
Available in Salesforce Classic in: **All** editions except Database.com

Salesforce1 Element	Available for Offline Use
Navigation Menu	Yes
Global Search	Previous searches only
Notifications	Previously viewed only
Feeds, Groups, and People	Previously viewed only
Salesforce Today	Main page and mobile event records if previously view
Salesforce Events	Previously viewed only

Salesforce1 Element	Available for Offline Use
Recent Objects	Yes (top five)
Other Objects	No
Record Details	Yes (30 most recent records)
Related Records	Previously viewed only
List Views	Previously viewed only
Tasks	Only tasks from the first page of the My Tasks list (up to 10 tasks), and only if the list was previously viewed or after the user manually updates the cache
Dashboards	Yes (top five)
Approvals (submit, approve, or reject)	No
Visualforce pages	No
Canvas Apps	No
Lightning Pages	No
Settings	Yes

Cached data is refreshed when a user switches to Salesforce1. If a user switches to another app, the user's cached data is automatically refreshed if the existing data store is over one hour old.

Users can manually cache their data at any time—for example, before switching into airplane mode or entering an area with no service. From the Salesforce1 navigation menu, select **Settings** > **Offline Cache** > **Cache Now**.



Note: The cache is saved for two weeks. Users can clear the cache by logging out of the Salesforce1 app.

Enable Visualforce Pages for the Salesforce1 Mobile App

You can use Visualforce to extend the Salesforce1 app and give your mobile users the functionality that they need while on the go. Before adding a Visualforce page to Salesforce1, 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 Salesforce1, 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 Salesforce1 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 for Salesforce1:

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 Salesforce mobile apps and Lightning Pages then click **Save**.

EDITIONS

Available in Lightning Experience in: **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 Salesforce1:

- "Customize Application"
  "Author Apex"

Consider these notes about Visualforce support in Salesforce1.

- Standard tabs, custom object tabs, and list views that are overridden with a Visualforce page aren't supported in Salesforce1. The Visualforce page is shown for full site users, but Salesforce1 users will see the default Salesforce1 page for the object. This restriction exists to maintain the Salesforce1 experience for objects.
- You can also enable Visualforce pages for Salesforce1 through the metadata API by editing the isAvailableInTouch field on the ApexPage object.
- The Salesforce Classic Mobile Ready checkbox on Visualforce Tab setup pages is for Salesforce Classic Mobile only and has no effect on Visualforce pages in the Salesforce1 apps.

SEE ALSO:

Customize the Salesforce1 Navigation Menu

Your Org's Branding in the Salesforce1 Mobile App

You can customize the Salesforce1 mobile 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 of the Salesforce1 apps.

Note: Images that you upload to customize the Salesforce1 app are stored in a Documents folder named Salesforce1 Branding Resources. For this reason, the Documents object must be enabled for your organization before administrators can view and modify the Salesforce1 Branding page. (The Documents tab doesn't need to be visible, however.)

For users of the Salesforce1 mobile browser app to see custom branding, Documents must be enabled for your organization. For the Salesforce1 downloadable apps, users must also have "Read" user permissions on Documents.

EDITIONS

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

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

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 Salesforce1 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 Salesforce1, 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.
- Salesforce1 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 Salesforce1 app icon that appears on the mobile device's home screen.
  - The initial loading screen when launching the Salesforce1 downloadable app 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 Salesforce1 app login page. My Domain must be enabled to modify the login page. To customize your company's Salesforce1 login page, see Customize Your Login Page Branding on page 570.

SEE ALSO:

Customize Branding of the Salesforce1 Mobile App

Customize Branding of the Salesforce1 Mobile App

Change the Salesforce1 mobile 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 Salesforce1 app are stored in a Documents folder named Salesforce1 Branding Resources. For this reason, the Documents object must be enabled for your organization before administrators can view and modify the Salesforce1 Branding page. (The Documents tab doesn't need to be visible, however.)

For users of the Salesforce1 mobile browser app to see custom branding, Documents must be enabled for your organization. For the Salesforce1 downloadable apps, users must also have "Read" user permissions on Documents.

1. From Setup, enter *Branding* in the Quick Find box, then select **Salesforce1 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**.

EDITIONS

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 Salesforce1 branding settings:
- "View Setup and Configuration"

To modify Salesforce1 branding settings:
- "Customize Application"

  "Modify All Data"

SEE ALSO:

Your Org's Branding in the Salesforce1 Mobile App

Salesforce1 Limits and Differences from the Full Salesforce Site

The Salesforce1 mobile app doesn't have all of the functionality of the full Salesforce site, and in some cases includes features that aren't available in the full site.

There are differences in these areas:

- Supported Salesforce data
- Page layouts (including fields and related lists)
- Navigation and actions
- Searching for information
- Creating and editing records
- Duplicate management
- Notes

- Salesforce Today
- Tasks and events
- Work.com features
- Salesforce1 Reporting
- Chatter feeds, topics, profiles, groups, and files
- Chatter Questions
- Salesforce Communities
- Approval requests
- Notifications
- Security
- Supported Salesforce customizations

Data Supported in Salesforce1: Limits and Differences from the Full Salesforce Site

These objects are available in the Salesforce1 mobile app:

- Accounts and Person Accounts
- Assets (*view or edit only in the downloadable apps*)
- Campaigns
- Cases
- Contacts
- Contracts
- D&B Company (*view only, for Data.com Premium Prospector and Data.com Premium Clean customers)*
- Dashboards (*view only*)
- Events
- Leads
- Live Chat Transcripts
- Opportunities
- Orders (*view or edit only*)
- Reports (*view only*)
- Salesforce Knowledge Articles (*view only*)
- Tasks
- Work.com Coaching, Goals, Thanks, Rewards, and Skills (*Skills not available in the iOS downloadable app*)
- Work Orders (*view or edit only in the downloadable apps*)
- Custom objects that have a tab you can access
- Lightning Connect external objects that are searchable and have a tab you can access

Note: To be available in Salesforce1, 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.

Salesforce1 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 Page Layouts in Salesforce1: Limits and Differences from the Full Salesforce Site for some issues with user fields in Salesforce1.

Salesforce1 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.

Accounts

- Social accounts:
  - You can't access social accounts features for LinkedIn, Facebook, Klout, or YouTube in Salesforce1.
  - If an account has been linked to a social network profile, the profile image selected for the account may display when viewing the account in Salesforce1 even when you aren't logged in to the social network. Profile images from LinkedIn appear when you're logged in to LinkedIn; 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 in Salesforce1.
  - You can view Tweets, retweets, replies, or favorites for an associated Twitter user if you're using a Salesforce1 downloadable app. With the Salesforce1 mobile browser app, tap the Twitter profile to see Tweets and so forth directly in Twitter. Also, in the Salesforce1 mobile browser app, you can't see who is following a Twitter user, or who the Twitter user is following.
  - Salesforce1 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 in Salesforce1, 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.
- Account News isn't available in the full Salesforce site.
- The **Delete** and **Manage External Account** buttons aren't available.
- You can't view the account hierarchy.
- You can't merge accounts or contacts.
- You can view account teams, 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.

Account Teams

- You can view account teams, but you can't add, edit, or delete account team members in Salesforce1.
- 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.

Cases

- Standard actions on Case Feed aren't supported in Salesforce1 and aren't available in the mobile app. Instead, quick actions provide the functionality. For example, to provide the Email action functionality on a case page, create a Send Email quick action and add it to the case page layout in Salesforce1 or the mobile app.

Standard Action Available in Salesforce Classic	Quick Action Available in Salesforce1 and Mobile App
Email	Send Email
Change Case Status	Update Case
Log a Call	Log a Call

  The **Portal** action is not supported Salesforce1 and isn't available in the mobile app.

  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 in the mobile app.

- Some fields on Service Contract and Contact Line Item related lists aren't available.
- These case related lists aren't available:
  - Business Hours on Holiday List
  - Case Contact Role
  - Milestone List
  - Solution List
  - Team Member List
  - Team Member on Team List
  - Team Template Member List

Contacts

- Social contacts:
  - You can't access social contacts features for LinkedIn, Facebook, Klout, or YouTube in Salesforce1.
  - If a contact has been linked to a social network profile, the profile image selected for the contact may display when viewing the contact in Salesforce1 even when you aren't logged in to the social network. Profile images from LinkedIn appear when you're logged in to LinkedIn; 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 in Salesforce1.
  - You can view Tweets, retweets, replies, or favorites for an associated Twitter user if you're using a Salesforce1 downloadable app. With the Salesforce1 mobile browser app, tap the Twitter profile to see Tweets and so forth directly in Twitter. Also, in the Salesforce1 mobile browser app, you can't see who is following a Twitter user, or who the Twitter user is following.
  - Salesforce1 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 in Salesforce1, you must add Twitter to the page layout for contacts. Access the full Salesforce site to edit page layouts.
- Activity logs aren't created when you use the  icon to send emails from the Salesforce1 app.
- The **Request Update**, **Manage External User**, and **Enable Customer User** buttons aren't available.

- You can't add opportunities, account users, or attachments on a contact, and you can't add a contact to a campaign.
- You can't merge accounts or contacts.
- You can't add contacts from Data.com or clean contact records with Data.com Clean.

Contracts

- The **Clone**, **Activate**, and **Deactivate** buttons aren't available.
- These contracts related lists aren't available:
  - Contract History
  - Items to Approve

Leads

- Social leads:
  - You can't access social leads features for LinkedIn, Facebook, Klout, or YouTube in Salesforce1.
  - If a lead has been linked to a social network profile, the profile image selected for the lead may display when viewing the lead in Salesforce1 even when you aren't logged in to the social network. Profile images from LinkedIn appear when you're logged in to LinkedIn; 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 in Salesforce1.
  - You can view Tweets, retweets, replies, or favorites for an associated Twitter user if you're using a Salesforce1 downloadable app. With the Salesforce1 mobile browser app, tap the Twitter profile to see Tweets and so forth directly in Twitter. Also, in the Salesforce1 mobile browser app, you can't see who is following a Twitter user, or who the Twitter user is following.
  - Salesforce1 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 in Salesforce1, 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.
- 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.

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
- The opportunity owner can't edit the `Probability` or `Forecast Category` fields. However, field values are automatically populated, based on the value of the `Stage Opportunities` field, when you save the record. The opportunity owner can manually edit the values for these fields in Salesforce Classic (but not from Lightning Experience).
- Before you can use Salesforce1 to add a product to an opportunity, the opportunity must already have a price book associated with it. You can associate the price book with an opportunity in the full Salesforce site only.
- You can't add products with revenue or quantity schedules to opportunities. If you do, the product appears on the opportunity, but the schedule is not created. You also can't re-establish a product schedule from an opportunity.

Opportunity Team

- The **Clone** and **Display Access** buttons aren't available.

Orders

- The **Create**, **Clone**, **Activate**, **Deactivate**, **Reduce Order** buttons aren't available.
- You can't add, edit, or remove order products.

Quotes

- Quote PDFs appear in the related list but aren't viewable.
- You can approve or reject quotes but you can't submit quotes for approval.
- You can't perform these actions:
  - **Email Quote**
  - **Create PDF**
  - **Start Sync**
  - **Stop Sync**

Salesforce Knowledge Articles

Articles aren't supported in the Salesforce1 downloadable app for iOS. Articles are supported in the Salesforce1 downloadable app for Android, version 8.0 or later and in the Salesforce1 mobile browser app, with these limitations:

Issue	Android Downloadable App, v8.0 or later	Mobile Browser App
Only published articles are available—not draft or archived articles.	●	●
Articles can't be created, edited, translated, or archived.	●	●

Issue	Android Downloadable App, v8.0 or later	Mobile Browser App
Articles can't be linked to cases. (But links that are set up from the full site can be viewed in Salesforce1 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. These features are available in all versions of Salesforce1 when searching from the Articles home page.	●	
Knowledge articles aren't available when accessing communities via the Salesforce1 mobile app.	●	●

Page Layouts in Salesforce1: Limits and Differences from the Full Salesforce Site

Fields

- While user detail pages aren't available in the Salesforce1 mobile app, user fields are supported and appear on user profiles, in related lists, and so forth.

  There are some issues when the following 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.

- These fields aren't supported in Salesforce1:
  - division fields
  - territory management fields

- Support for rich text area fields varies by the version of Salesforce1 and the type of device.

Device	Salesforce1 Version	View Rich Text Area Fields	Edit Rich Text Area Fields
Android	Downloadable App Mobile Browser App	Yes	Yes The rich text editor isn't available. But you can manually add HTML tags.
BlackBerry	Mobile Browser App	No	No
iOS	Downloadable App	Yes	No
iOS	Mobile Browser App	Yes	Yes The rich text editor is available.
Windows 8.1	Mobile Browser App	No	No

Tab-Key Order on Page Layouts

- The top-down tab-key order isn't supported in Salesforce1. Even if a page layout is configured to allow users to move through fields in a top-down order, Salesforce1 moves through fields in a left-to-right order only.

Related Lists

- Related lists in Salesforce1 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 Data Supported in Salesforce1: Limits and Differences from the Full Salesforce Site on page 730 for related lists that aren't available for specific objects.
- The Notes and Attachments related list isn't fully supported in Salesforce1. There are several issues, including:
  - Attachments added in the full Salesforce site aren't guaranteed to open in Salesforce1, 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 in Salesforce1.
  - 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 Salesforce1 action bar. Depending on how your administrator has configured Notes in Salesforce1, 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.

Navigation and Actions in Salesforce1: Limits and Differences from the Full Salesforce Site

Navigation

- The Salesforce1 mobile app is supported in portrait orientation only. In the downloadable apps, the interface doesn't rotate when a device is switched to landscape orientation. The mobile browser app interface does rotate but isn't guaranteed to work correctly in this orientation.

Actions

- Most actions, including quick actions, productivity actions,and standard and custom buttons, are displayed in the action bar or list item actions in Salesforce1.
- 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 in Salesforce1: Limits and Differences from the Full Salesforce Site

In Salesforce1, you don't search across multiple objects at the same time when doing a global search. Instead, you use the search scope bar beneath the global search box to pick the object that you want to search.

The objects available in the search scope bar are the same as the items that appear in the Recent section of the Salesforce1 navigation menu. If you're new to Salesforce and don't yet have a history of recent objects, you're able to search the default set of objects: Accounts, Cases, Contacts, Files, Leads, Opportunities, and Groups and People (unless these items were added directly to the navigation menu). As you spend time working in Salesforce1 and the full Salesforce site, 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 Salesforce1.

If a desired object isn't yet available via global search in Salesforce1, you can search the object directly. From the navigation menu, tap **More** beneath the Recent section to see all objects available to you. Then tap the object to open it's record search page.

List views aren't included in Salesforce1 search results, from either a global search or an object-specific record search. To find list views, 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.

Lookups only search the name field for each object.

When searching in Salesforce1, you can't:

- Filter search results
- Pin frequently used items
- Search by division

Data Entry in Salesforce1: Limits and Differences from the Full Salesforce Site

There are some differences between the full Salesforce site and the Salesforce1 app when you're adding new records or updating existing data.

Category	Issue	Creating Records	Editing Records
Any Record	Inline editing isn't available.	✔	✔
	You can't modify a record's owner or its record type.		✔

Category	Issue	Creating Records	Editing Records
	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	An event owner can't change, add, or remove an event's invitees. 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.	✔	✔
	Proposed Events (the **New Meeting Request** button) aren't supported.	✔	✔
	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.	✔	✔
	Spell-checking for the `Description` field isn't available.	✔	✔
	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 `Probability` or `Forecast Category` fields. However, values are automatically added to these fields (based on the value of the `Stage` field) when you save the record. You can manually edit the values for these fields in the full site.	✔	✔
Tasks	The `Subject` field doesn't include a picklist of previously defined subjects.	✔	✔
	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.	✔	✔

Category	Issue	Creating Records	Editing Records
	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 or change the details of a recurring task series. (You can change the details of individual occurrences in a task series.)	✔	✔
	Spell-checking for the `Comments` fields isn't available.	✔	✔
	You can't add attachments.	✔	✔
	You can't send notification emails.	✔	✔
	You can't set task reminders.	✔	✔
Lookup Fields	Administrator-defined dependent lookup filters aren't supported.	✔	✔
	User-defined lookup filter fields aren't supported.	✔	✔
Phone Number Fields	Phone number fields display a keypad, from which you tap out the phone number. The keypad doesn't include parentheses, hyphens, or periods, and Salesforce1 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.	✔	✔
Picklist Fields	Controlling and dependent picklists are supported, but Salesforce1 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.	✔	✔

Duplicate Management in Salesforce1: Limits and Differences from the Full Salesforce Site

Duplicate management in the Salesforce1 app is similar to the full site, with these differences:

- Each possible duplicate is shown on a "duplicate card." Salesforce1 shows 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 the organization, not from the associated matching rule.
- You can tap a duplicate card to view the possible duplicate record's complete details, but that action erases the information you entered in the new or updated record. You must re-enter that information before you can save the record or view additional duplicate cards.
- By default, duplicate rules run when you complete fields on a record. In Salesforce Classic, duplicate rules run when you save a record.

Notes in Salesforce1: Limits and Differences from the Full Salesforce Site

- When using Salesforce1, you can access all of your notes from the **Notes** item in the Salesforce1 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 relate a note to multiple records in the Salesforce Classic version of the full site, but you can do this using the mobile app.

Salesforce Today in Salesforce1: Limits

The Salesforce Today app is available in the Salesforce1 downloadable apps for Android phones and iPhone and iPad devices. It's not available in the Salesforce1 mobile browser app, 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.
- On devices running Android 4.4, weather information is always displayed in Today, even if access to location information is disabled. This is an Android 4.4 issue and not something that Today can control.
- 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 in Salesforce1: Limits and Differences from the Full Salesforce Site

Events

- Archived events aren't available.
- You can't use Shared Activities to relate multiple objects to an event.
- You can't add events to Microsoft® Outlook®.
- You can't add invitees to events or remove them from events.
- You can't accept or decline an event you've been invited to.
- The Recurrence and Reminder sections aren't displayed on event detail or edit pages.
- Events respect your Salesforce time zone settings, not the time zone setting on your mobile device.
- When viewing Salesforce events from the **Events** item in the Salesforce1 navigation menu, the date bar always begins on Sunday and ends on Saturday, regardless of your device and Salesforce locale settings.
- If viewing the current day's event list at 11:59pm, the list doesn't automatically refresh to the next day at Midnight.

- Invitee related lists display slightly different content from the full Salesforce site. In the full site, the Invitee list includes the event owner as well as invitees. In Salesforce1, the Invitee related list includes invitees only. The following queries let you reproduce the full site functionality in Salesforce1.

  If you use Shared Activities in your organization, to allow the event organizer to see all the invitees, use this query:

  ```
  SELECT RelationId FROM EventRelation WHERE isInvitee = true AND eventId='[Event_Id]'
  ```

  where *Event_Id* is the child event's ID.

  To allow the event organizer to see all the invitees if your organization doesn't use Shared Activities, use this query:

  ```
  SELECT RelationId FROM EventRelation WHERE eventId='[Event_Id]'
  ```

  These queries get the main event's relations and display them for the given child event. You can add a `WHERE` clause to further filter the results.

Tasks

- Only the **My Tasks**, **Completed Within Last 7 Days**, **Delegated**, and **Today** task lists are available for the Tasks item in Salesforce1. All other task lists, including **Overdue**, **This Month**, and **All Open**, aren't available in the mobile app.
- Archived tasks aren't available.
- You can't use Shared Activities to relate multiple contacts to a task.
- Group (multiuser) tasks aren't available.
- The Recurrence and Reminder sections aren't displayed on task detail or edit pages.
- When you close a task by tapping the ☐ icon, the task is shown crossed out until you refresh the list.
- In task lists, the sorting of priority tasks is determined by the order of the fields in the priority picklist.
- The more tasks that you have, and the more relationships that your tasks have to other records, the longer it may take to view tasks or use other features in the Salesforce1 app.
- When more than 1,000 overdue tasks exist, task lists in Salesforce1 don't display any overdue tasks at all. Use the full site to view your overdue tasks and close them, postpone them, or delete their due dates.
- 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).
  - All tasks show the subject.
  - All tasks show the due date, if it exists and a user has permission to view it.
  - Tasks include the primary contact and the account or other record, if they exist.

  The fields in each list may vary, depending on your organization's settings.

  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 subject or due date field to either layout doesn't change the appearance of tasks—those fields won't appear twice.

  Below the built-in task elements, Salesforce1 displays up to three additional 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.

Work.com in Salesforce1: Limits and Differences from the Full Salesforce Site

When using Work.com features in Salesforce1, 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

Reports and Dashboards in Salesforce1: Limits and Differences from the Full Salesforce Site

Reports

Feature	Notes about Salesforce1 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 in Salesforce1, 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 in Salesforce1.
Filters	When you open a report from the Reports tab, you can't filter the report. But, when you tap a dashboard component to open the source report, if the source report is a summary or matrix report, you can filter the report by tapping a value on the chart. If the report is a tabular or joined report, then you can't filter it. Row limit filters aren't available.
Custom Summary Formula Fields	Custom summary formula fields don't display in Salesforce1.

Other Notes about Using Reports in Salesforce1

- You can't drill into reports that have more than three checkbox fields.
- When you view a report with more than 16 summary fields in Salesforce1, you receive an error message.
- Salesforce1 can't render reports via URLs that use dynamic parameter values. If you modify a URL to pass parameters into reports, Salesforce1 shows a blank screen (a report record with no returned results).

Dashboards

Feature	Notes about Salesforce1 Availability
Edit a Dashboard	You can't edit dashboards in Salesforce1. Dashboards are read-only.
Refresh a Dashboard	In addition to rerunning all reports in a dashboard, which can take time, you can quickly refresh the dashboard to show data from the last run.
View As	In Salesforce1, as in the full Salesforce site, you can only run dashboards as a user in your role hierarchy. However, in Salesforce1 you can choose from all users in your organization. If you select a user outside your role hierarchy, you get an error.
Lightning Experience Dashboard Layout	Lightning Experience dashboards that have more than three columns display in a three-column layout on phones and tablets.

Other Notes about Using Dashboards in Salesforce1

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. In Salesforce1, you see the report and the dashboard chart on the same page.

Charts

Other Notes about Using Charts in Salesforce1

- Unless you turn on **Enable Enhanced Charts in Salesforce1**, legacy Salesforce Classic charts display instead of the new Lightning Experience charts. After turning on **Enable Enhanced Charts in Salesforce1**, all users see enhanced charts regardless of whether or not they switch to Lightning Experience on the full Salesforce site.
- Enhanced charts are very similar to Lightning Experience charts, but they have the following limitations:
  - Scatter, and table charts aren't supported and appear as horizontal bar charts. Cumulative line charts aren't supported and appear as line charts.
  - Enhanced charts show only the first 100 groupings in the default sort order.
  - You can't post enhanced charts to Chatter.
  - When you open Salesforce1, dashboards aren't automatically stored on your device for offline viewing. However, when you view a dashboard, it's saved in your device's cache so you can view it offline later.

- Report Charts aren't available.

Chatter in Salesforce1: Limits and Differences from the Full Salesforce Site

When using Chatter in the Salesforce1 mobile app, you can't:

Feeds

- Send or view Chatter messages.
- See Chatter activity statistics or Chatter influence status.
- Share public posts.
- Add or view Chatter favorites.
- Filter records.
- Search in feeds on user profiles and records.
- Invite coworkers to sign up for Chatter.
- Use emoticons, the character combinations that add expressions like a smiley face to a post.
- Edit feed posts or comments (but you can see feed items that were edited in the full site).

Topics (Salesforce1 mobile browser app only)

- See trending topics.
- Edit topic details (name and description).
- Tag favorite topics.
- See a large list of tagged topics all at once—tap **More** to see all 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.

People and Profiles

- Edit profile information in the Salesforce1 downloadable app for iOS devices.
- Upload a profile photo using the Good Access™ secure mobile browser.
- Use custom profiles.

Groups

- Invite customers to join private customer groups.
- Add records to Chatter groups with customers using the Add Record publisher action.
- Withdraw requests to join private groups
- Change email and in-app notification settings for groups in communities.
- Perform the following group owner and manager actions:
  - Remove files from the group files list.
  - Upload group photos from the Salesforce1 downloadable apps

Chatter Messenger

- Chat with people.
- View your chat history.

Files

- View file types other than these: `.doc`, `.docx`, `.pdf`, `.ppt`, `.pptx`, `.xls`, `.xlsx`, and all image files, including `.gif`, `.jpg`, and `.png` formats.
- Access Files from the Salesforce1 navigation menu if you're a high-volume portal user.
- Upload files using the Good Access secure mobile browser.

Chatter Questions in Salesforce1: Limits and Differences from the Full Salesforce Site

- To access the action drop-down menu for a question, tap the question.
- You don't see similar questions and knowledge articles when you ask questions.
- You can't select best answers.

Salesforce Communities in Salesforce1: Limits and Differences from the Full Salesforce Site

Salesforce Communities in Salesforce1 is similar to the full site, with these differences:

- The Salesforce1 navigation menu in a community is different from the navigation menu in your internal organization in the following ways:
  - The navigation menu shows only the tabs that the administrator has included in that community via Tabs & Pages in the community's administration settings.
  - The Chatter tab is divided into three menu options in Salesforce1. If your community includes the Chatter tab, you'll see navigation menu items for Feeds, People, and Groups.
  - The Events and Today items aren't supported in communities when accessed via Salesforce1; these items don't display in the navigation menu.
  - Tasks are available only to users with the Edit Tasks permission.
  - Salesforce Knowledge articles aren't supported in communities when accessed via Salesforce1; this item doesn't display in the navigation menu.
- There is no All Company Feed.
- Site.com branding is not supported.
- The Community Management page isn't available in Salesforce1.
- Community members can't flag private messages as inappropriate.
- Reputation isn't supported in Salesforce1. However, if reputation is enabled and set up in the full site, users do accrue points when using Salesforce1. For example, if the community manager set up a point system in the full site and assigned point values for writing a post and commenting on a post, then users in the community earn points with every post and comment made in Salesforce1. Users can view their points in the full site only though.
- Search is scoped by community and returns only items from the current community. The only exception is records, since they are shared across communities.
- 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 Salesforce1 Mobile Browser App, external users' photos don't include any visual indication that the user is an external user. In the full Salesforce site and Salesforce1 Downloadable App, the upper left corner of an external user's photo is orange.

- In the Salesforce1 Mobile Browser App, 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 Salesforce1 Downloadable App, photos appear next to users' names in the People list.
- The community template and your user licenses determine how you can access communities using Salesforce1. For more information, see *Access to Communities Using Salesforce1* in the Salesforce Help.
- Salesforce Knowledge is not supported for communities in the Salesforce1 mobile browser app and the Salesforce1 downloadable apps for iOS and Android.
- Group members in communities can't edit their email and in-app notification settings in Salesforce1. As a workaround, users can set their group email notification preference to **Every Post** in the community from the full site. Doing this automatically enables both email notifications and in-app notifications in Salesforce1 for that group.

Approvals in Salesforce1: Limits and Differences from the Full Salesforce Site

These approval-related options aren't available in the Salesforce1 mobile app:

- Recalling approval requests.
- Reassigning approval requests.
- Manually selecting the next approver. For approval requests that require this manual selection, the approver needs to log in to the full Salesforce site.

In addition:

- The Approval History related list doesn't display comments.
- Salesforce1 notifications for approval requests aren't sent to queues. For each approval step involving a queue, we recommend adding 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.
- Salesforce1 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 won't be able to complete the approval request until someone grants record access.
- 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.

Salesforce1 Notifications: Limits

- The notifications list in the app displays the 20 most recent notifications you received within the last 90 days.
- To ensure that sensitive information isn't distributed through a third-party service without proper authorization, push notifications include only minimal content by default. To include full content in push notifications (for example, a post or a comment, a Chatter group's name, or a task description), from Setup in the full site, enter `Salesforce1 Notifications` in the `Quick Find` box, then select **Salesforce1 Notifications**. Next, select `Enable full content in push notifications`, and agree to the terms and conditions on behalf of your company.
- The Salesforce1 mobile browser app uses the Streaming API. Streaming API limits apply to in-app notifications in the mobile browser app.
- When you submit a record for approval in Salesforce, you can add comments. These comments are included in the approval process step detail page in Salesforce. In Salesforce1, you cannot view comments when you look at approval details.

Security in Salesforce1: Limits and Differences from the Full Salesforce Site

When a user who doesn't have the "View Encrypted Data" permission clones a record, encrypted fields show masked data.

Salesforce Customizations in Salesforce1: Limits and Differences from the Full Salesforce Site

Custom Home Pages

- Salesforce1 doesn't support login redirection to 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 from a mobile browser, turn off the Salesforce1 mobile browser app. 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 Salesforce1. Remember that Visualforce pages must be enabled for use in Salesforce1.

  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 Salesforce1.

- Custom images used for action icons must be less than 1 MB in size.
- 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 in Salesforce1.

Visualforce Pages

- Standard tabs, custom object tabs, and list views that are overridden with a Visualforce page aren't supported in Salesforce1. The Visualforce page is shown for full site users but Salesforce1 users will see the default Salesforce1 page for the object instead. This restriction exists to maintain the Salesforce1 experience for objects.
- Embedded Visualforce pages—that is, those added to a page layout—that contain an `<apex:enhancedList>` component may cause the Salesforce1 app to crash when used on iOS devices.
- When viewing Visualforce pages on an Android device, horizontal scrolling doesn't work if the page is wider than the viewport. Redesign the page so that it's narrower than the viewport.

Lightning Pages

- You can't add more than 25 components to a Lightning Page.

Programmatic Customizations

- These programmatic customizations to the UI aren't supported: Web tabs and S-controls.

SalesforceA

Manage users and view information for Salesforce organizations from your mobile device.

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.

Overview of Your Organization

The Overview screen shows:

- Number of frozen and locked out users
- Trust status
- Recently viewed users

EDITIONS

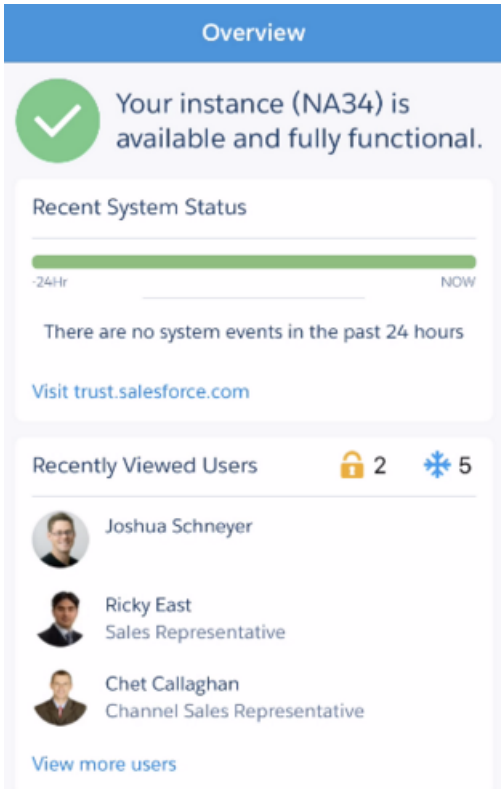
Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To use SalesforceA:

- "Manage Users"



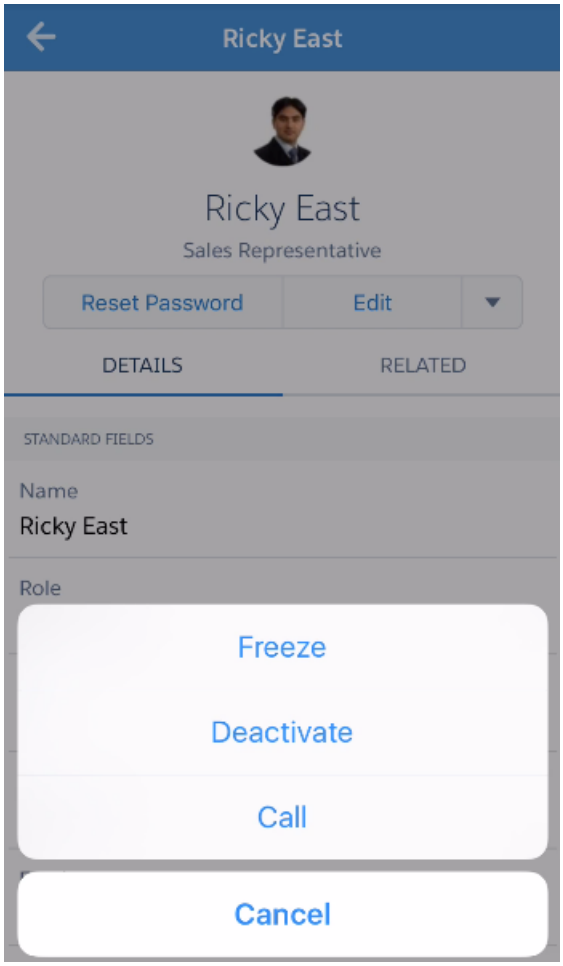
For Android users, the navigation icon is in the top left. Tap it to go to the navigation menu.

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



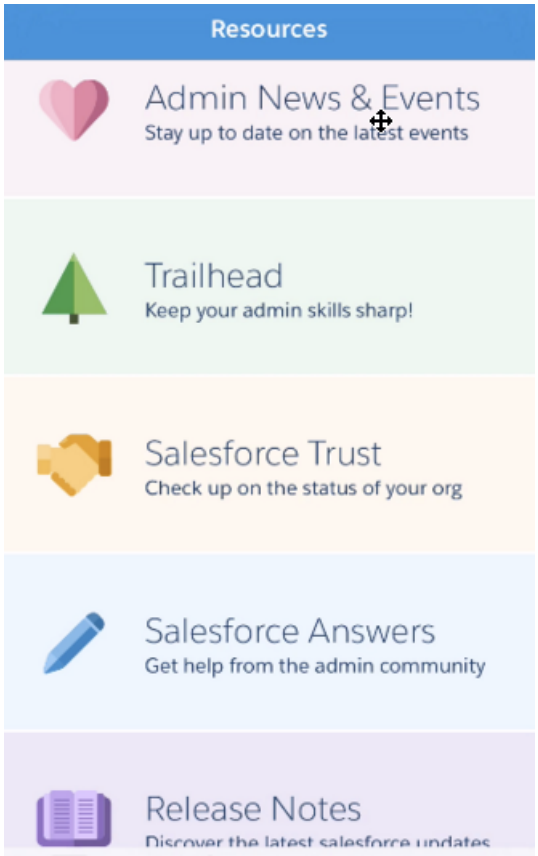
Swipe to the Related page to see:

- The user's current permission sets
- The user's login history

Additional Information

The Resources page gives you quick access to:

- Admin news and events
- Trailhead
- Salesforce trust
- Salesforce answers
- Salesforce release notes



SEE ALSO:

Log In to SalesforceA

Log In to Multiple Organizations with SalesforceA

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

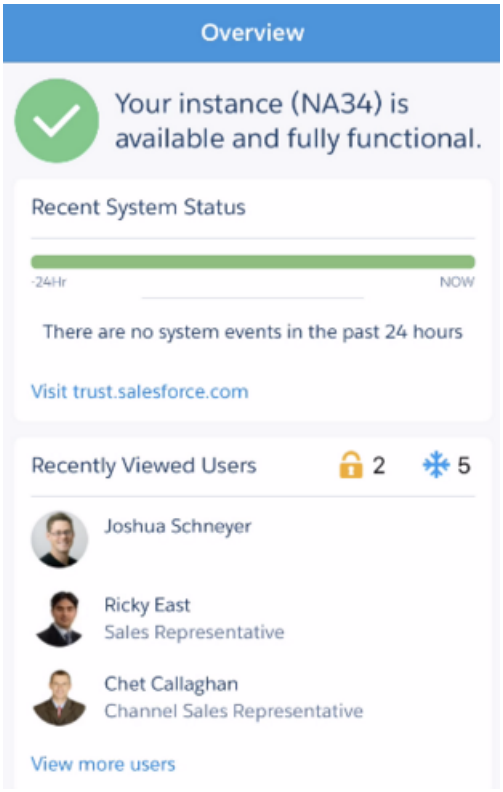
Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To use SalesforceA:

- "Manage Users"



SEE ALSO:

SalesforceA

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

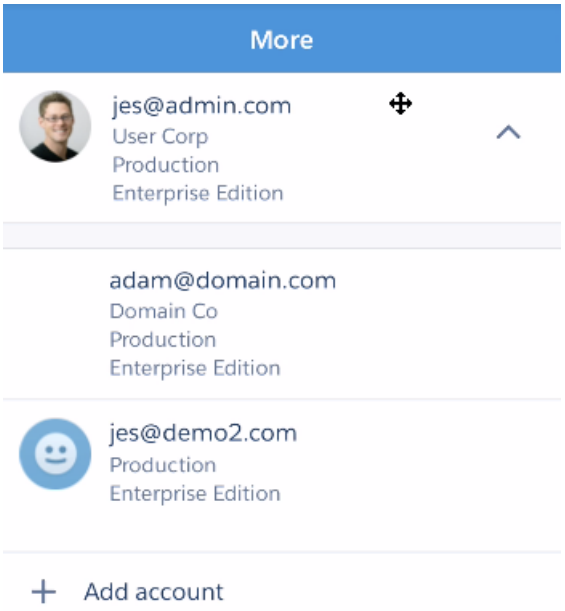
Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To use SalesforceA:

- "Manage Users"



SEE ALSO:

SalesforceA

Salesforce Classic

Salesforce Classic Mobile Overview for Administrators

Salesforce Classic Mobile helps your teams succeed by allowing users to access their latest Salesforce data, whenever and wherever they need it, directly from Android™, BlackBerry® and iPhone® devices. The Salesforce Classic Mobile 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 Classic Mobile license is required for each user to use the full version of Salesforce Classic Mobile. For organizations using Unlimited, Performance, and Developer Editions, Salesforce provides one mobile license for each Salesforce license. Organizations using Professional or Enterprise Editions must purchase mobile licenses separately.

Any Salesforce user who doesn't have a mobile license can download a free, restricted version of Salesforce Classic Mobile. The free version:

- Supports fewer standard objects
- Doesn't support custom objects
- Doesn't allow administrators to customize or create mobile configurations
- Isn't available for use by partner portal users

Note: The Android, BlackBerry, and iPhone apps are available in English, Japanese, French, German, and Spanish. Contact Salesforce to turn on Salesforce Classic Mobile for your organization.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

SEE ALSO:

Setting Up Salesforce Classic Mobile
Salesforce Classic Implementation Guide
Salesforce Classic User Guide for BlackBerry
Salesforce Classic User Guide for iPhone

About the Salesforce Classic Mobile Default Configuration

Mobile configurations for the Salesforce Classic Mobile 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 Classic Mobile app.

The default mobile configuration:

- Allows users with an assigned mobile license to install and activate Salesforce Classic Mobile, even if you haven't yet assigned them to a mobile configuration.
- Allows users without an assigned mobile license to install and activate the free version of Salesforce Classic Mobile.

You can disable Salesforce Classic Mobile to prevent users from activating the Salesforce Classic Mobile 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 Classic Mobile app are mobilized with the default configuration.
- Assets aren't available as a tab in the Salesforce Classic Mobile app but display as a related list for accounts, cases, and contacts.

The default configuration automatically synchronizes records the user recently accessed in Salesforce on the Salesforce Classic Mobile 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

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

Salesforce Classic Mobile Implementation Tips and Best Practices

Set up the Salesforce Classic Mobile app using these tips and best practices.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile configurations:
- "View Setup and Configuration"

To create, change, or delete Salesforce Classic Mobile 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 Classic Mobile 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 Classic Mobile 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 Classic Mobile 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 Classic Mobile app. Salesforce Classic Mobile 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 Classic Mobile 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 Classic Mobile app. For example, Salesforce Classic Mobile 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 Classic Mobile 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 Classic Mobile 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 Classic Mobile app in the sandbox before deploying to your organization.
- Use of the Salesforce Classic Mobile app requires a data plan. The wireless data volume for the Salesforce Classic Mobile 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 Classic Mobile 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 Classic Mobile app is low compared to moderate email usage.

- If you're deploying to BlackBerry users, evaluate your corporate network infrastructure before implementing the mobile solution.

Best Practices

- Use the zero-administration deployment option to experiment with the Salesforce Classic Mobile app before you set up mobile configurations. You'll create better blueprints for your mobile configurations if you've tried using the Salesforce Classic Mobile 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 Classic Mobile 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 Classic Mobile

To deploy the Salesforce Classic Mobile 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 dashboards (optional)
10. Set up mobile reports (optional)
11. Set up Salesforce CRM Content (optional)
12. Configure access for partner users (optional)
13. Create links to Web and Visualforce Mobile pages (optional)
14. Notify users that Salesforce Classic Mobile is available for download

When users download the Salesforce Classic Mobile app and activate their accounts, you can manage their devices in the Salesforce Classic Mobile Administration Console.

SEE ALSO:

Manage Salesforce Classic Mobile Configurations

Manage Salesforce Classic Mobile Devices

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile settings:

- "View Setup and Configuration"

To change Salesforce Classic Mobile settings:

- "Manage Mobile Configurations"

Enabling Salesforce Classic Mobile Users

To enable users to access to the full version of Salesforce Classic Mobile:

1. Allocate mobile licenses to users by selecting the `Salesforce Classic Mobile User` checkbox on the user record.
2. Edit each custom profile to which Salesforce Classic Mobile users are assigned to include the "API Enabled" permission. Salesforce Classic Mobile 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, BlackBerry, and iPhone apps are available in English, Japanese, French, German, and Spanish. Contact Salesforce to turn on Salesforce Classic Mobile for your organization.

To prevent users from activating the full version of Salesforce Classic Mobile on their mobile devices before you're ready to deploy the app, disable the `Salesforce Classic Mobile 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 Classic Mobile is enabled by default. If you want to block users without Salesforce Classic Mobile licenses from accessing their Salesforce data on mobile devices, disable the free version of Salesforce Classic Mobile.

1. From Setup, enter *`Salesforce Classic Settings`* in the `Quick Find` box, then select **Salesforce Classic Settings**.
2. Click **Edit**.
3. Deselect `Enable Mobile Lite`.

   Note: If you deselect this option while users are running the Salesforce Classic Mobile app, the Salesforce data on their devices is erased the next time the devices synchronize with Salesforce.

4. Click **Save**.

SEE ALSO:

Salesforce Classic Implementation Guide
Salesforce Classic User Guide for BlackBerry
Salesforce Classic User Guide for iPhone
Setting Up Salesforce Classic Mobile

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile settings:
- "View Setup and Configuration"

To change Salesforce Classic Mobile settings:
- "Manage Mobile Configurations"

Create Salesforce Classic Mobile 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.Any Salesforce user who doesn't have a mobile license can download a free, restricted version of Salesforce Classic Mobile. These users are assigned to the default mobile configuration when they activate their Salesforce account from a mobile device.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile configurations:

- "View Setup and Configuration"

To create, change, or delete Salesforce Classic Mobile 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 Classic Mobile 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 Classic Mobile Configurations
- Define Data Sets
- Setting Up Salesforce Classic Mobile

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

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

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 Classic Mobile for Android. Salesforce Classic Mobile for iPhone and BlackBerry don't currently support attachments.
   - Salesforce Classic Mobile 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 Classic Mobile.

   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:

- Salesforce Classic Mobile Overview for Administrators
- Manage Salesforce Classic Mobile Configurations
- Setting Up Salesforce Classic Mobile

Merge Fields for Mobile Filter Criteria

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:

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

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

Merge Field	Description
	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.

SEE ALSO:

- Manage Salesforce Classic Mobile Configurations
- Salesforce Classic Mobile Overview for Administrators
- 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:

- Salesforce Classic Mobile Overview for Administrators
- Manage Salesforce Classic Mobile Configurations
- Define Data Sets

Test Salesforce Classic Mobile Configurations

When you create a Salesforce Classic Mobile 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.

      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**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile data sets:

- "View Setup and Configuration"

To test Salesforce Classic Mobile configurations:

- "Manage Mobile Configurations"

    - On a BlackBerry device, open the menu and select **System Info**, then open the menu and select **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:

Salesforce Classic Mobile Overview for Administrators

Manage Salesforce Classic Mobile Configurations

Manage Salesforce Classic Mobile Devices

Setting Up Salesforce Classic Mobile

Edit Object Properties for Salesforce Classic Mobile

You can change the properties of standard and custom objects in the Salesforce Classic Mobile app. For example, you can restrict the permissions of Salesforce Classic Mobile users, or you can exclude unnecessary fields from the object's mobile page layout.

Salesforce Classic Mobile 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 Classic Mobile Page Layouts
5. Click **Save**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile configurations:
- "View Setup and Configuration"

To edit Salesforce Classic Mobile object properties:
- "Manage Mobile Configurations"

Remove Mobile Permissions

The Salesforce Classic Mobile 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 Classic Mobile, 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 Classic Mobile 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 Classic Mobile doesn't support all Salesforce features, such as S-controls and Apex. If your business process for an object is unsupported by Salesforce Classic Mobile, 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 Classic Mobile.

Note: Currently, you can't block mobile permissions for the content object.

Customize Salesforce Classic Mobile Page Layouts

The Salesforce Classic Mobile 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 Classic Mobile 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 Classic Mobile 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:

Salesforce Classic Mobile Overview for Administrators

Manage Salesforce Classic Mobile Configurations

Manage Salesforce Classic Mobile Tabs

Create Links to Web and Visualforce Mobile Pages for Salesforce Classic Mobile

Setting Up Salesforce Classic Mobile

Assign Tabs to a Salesforce Classic Mobile Configuration

For each mobile configuration, you can select the tabs that appear in the Salesforce Classic Mobile 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 Classic Mobile

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 Classic Mobile app.

By default, tabs work the same in the Salesforce Classic Mobile app as in the full Salesforce site—if an object's tab is hidden in Salesforce, it's hidden in Salesforce Classic Mobile 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 Classic Mobile app if users have permission to view the tab.

There are several reasons you might want to hide an object's tab in Salesforce Classic Mobile even though the object records are sent to the device. The Salesforce Classic Mobile 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**.
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 Classic Mobile app.
5. Click **Save**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile configurations:

- "View Setup and Configuration"

To customize Salesforce Classic Mobile tabs:

- "Manage Mobile Configurations"

Note: iPhone users can customize the order of their tabs in the Salesforce Classic Mobile 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 Classic Mobile Tabs
- Enabling Web and Visualforce Tabs for Salesforce Classic Mobile
- Salesforce Classic Mobile Overview for Administrators
- Manage Salesforce Classic Mobile Configurations

Enabling Web and Visualforce Tabs for Salesforce Classic Mobile

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

You can make web and Visualforce tabs available in the Salesforce Classic Mobile app. When you build the web tab or Visualforce tab, edit the tab properties and select the `Salesforce Classic Mobile 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 Classic Mobile 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 Classic Mobile app:

- The ability to mobilize web tabs is only available for BlackBerry and iPhone devices. If you mobilize a web tab, keep in mind that Android users can't view the tab in Salesforce Classic Mobile.
- The minimum BlackBerry operating system requirement for web tabs is 4.3.
- 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.
  - The BlackBerry browser has limited support for JavaScript and no support for 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, both iPhones and BlackBerry smartphones—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.
- JavaScript must be enabled on BlackBerry devices in order to view JavaScript web pages. The BlackBerry administrator can globally enable JavaScript from the BlackBerry Enterprise Server. Users can also enable JavaScript on a BlackBerry smartphone by opening the BlackBerry browser, selecting **Options** > **Browser Configuration**, and then selecting the **Support JavaScript** checkbox.

Visualforce Mobile Tab Considerations

Consider the following when defining a mobile Visualforce tab:

- Visualforce Mobile is only available for BlackBerry and iPhone. If you mobilize a Visualforce tab, keep in mind that Android users can't view the tab in Salesforce Classic Mobile.
- The Salesforce Classic Mobile app can run on BlackBerry operating system versions 4.3 through 7.0. For optimum performance, however, Salesforce recommends running Visualforce Mobile on BlackBerry smartphones installed with at least version 6.0.
- 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. Additionally, most BlackBerry browsers older than the 6.0 OS can't properly interpret CSS . 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 Classic Mobile app.
- In the Salesforce Classic Mobile 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. JavaScript must be enabled on BlackBerry devices in order to view Visualforce pages. The BlackBerry administrator can globally enable JavaScript from the BlackBerry Enterprise Server. Users can also enable JavaScript on a BlackBerry smartphone by opening the BlackBerry browser, selecting **Options** > **Browser Configuration**, and then selecting the **Support JavaScript** checkbox.
- The embedded browser in the BlackBerry client application doesn't have built-in navigation. If your Visualforce page is a wizard, you should provide navigation links that allow users to return to the previous page and advance to the next page.
- BlackBerry administrators should be aware that the download size setting on the BlackBerry Enterprise Server affects how much data can be pushed to the device. Check that the download size setting is appropriate, and be sure to test your Visualforce pages before deploying them to your Salesforce Classic Mobile users.
- 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 Classic Mobile Tabs

Manage Salesforce Classic Mobile Configurations

Create Links to Web and Visualforce Mobile Pages for Salesforce Classic Mobile

Assign Tabs to a Salesforce Classic Mobile Configuration

Create List Views for Salesforce Classic Mobile

You can create custom list views for Salesforce Classic Mobile users. Custom list views for Salesforce Classic Mobile, 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 Classic Mobile:

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

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile devices and users:

- "View Setup and Configuration"

To manage Salesforce Classic Mobile 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.
   a. 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.
   b. Set the sort order to Ascending or Descending.

8. Click **Save**.

SEE ALSO:

Manage Salesforce Classic Mobile Views
Manage Salesforce Classic Mobile Configurations
Manage Salesforce Classic Mobile Devices
Setting Up Salesforce Classic Mobile

Set Up The Mobile Dashboards for iPad App

Important: As of Summer '15, the Mobile Dashboards for iPad app is no longer supported. You can continue to use the app, but Salesforce no longer provides support in the form of bug fixes or enhancements for any issues you may encounter. Talk to your Salesforce administrator about migrating to the Salesforce1 app, the new Salesforce mobile experience.

You can make the Dashboards tab available in Salesforce Classic Mobile by adding it to the tabs for a mobile configuration. Mobile dashboards allow field users to keep up with corporate metrics and key performance indicators even when they are away from their desks.

Note the following about mobile dashboards:

- The Dashboards tab in the mobile application launches an embedded browser to display the dashboards.
- Due to screen size limitations, mobile dashboards display in a single column.
- Links to custom report details are disabled in mobile dashboards.
- The first time a user visits the Dashboards tab in Salesforce Classic Mobile, the mobile application requests the last dashboard the user viewed in Salesforce. Depending on the strength of the cellular or WiFi signal, it could take several minutes before the dashboard displays on the page.
- Dashboards do not automatically refresh in the mobile application. Users can request a dashboard refresh by clicking the **Refresh** button.
- Users are able to work offline in the mobile application. Without a wireless connection, users can see the last viewed dashboard, but they cannot refresh the dashboard or select a different one.
- The minimum BlackBerry operating system requirement for mobile dashboards is 4.5. Mobile dashboards are compatible with version 4.3, but tables in the dashboards might not display properly.
- BlackBerry administrators should be aware that the download size setting on the BlackBerry Enterprise Server affects how much dashboard data can be pushed to the device. Check that the download size setting is appropriate, and be sure to test your dashboards before deploying them to your mobile users.

Note: Currently, dashboards are only available in the BlackBerry and iPhone mobile client applications.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To view mobile configurations:
- "View Setup and Configuration"

To mobilize dashboards:
- "Manage Mobile Configurations"

To enable mobile dashboards:

1. From Setup, enter *Mobile Dashboards* in the Quick Find box, then select **Mobile Dashboard Settings**. 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**.
3. Select **Dashboards** from the Available Tabs list, and 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 mobile application, not just the Dashboards tab.
4. In the Selected Tabs list, choose the Dashboards tab and click the **Up** and **Down** arrows to define where the Dashboards tab should appear in the mobile application.
5. Click **Save**.

SEE ALSO:

Setting Up Salesforce Classic Mobile

Enable Reports in Salesforce Classic Mobile

To enable reports in the Salesforce Classic Mobile 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 Classic Mobile 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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To create, edit, and delete public report folders:
- "Manage Public Reports"

To view Salesforce Classic Mobile configurations:
- "View Setup and Configuration"

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 Classic Mobile, 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 Classic Mobile app.
12. Click **Save**.

Note: Currently, reports in Salesforce Classic Mobile aren't available on Android or iPhone devices.

SEE ALSO:

Setting Up Salesforce Classic Mobile

Setting Up Salesforce CRM Content for Salesforce Classic Mobile

Note the following about how Salesforce CRM Content is implemented in Salesforce Classic Mobile:

- 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 Classic Mobile is only supported on BlackBerry and iPhone devices.
- Content is not available in the free version of Salesforce Classic Mobile.
- You can't block mobile permissions for the content object. Currently, the content object in Salesforce Classic Mobile 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 Classic Mobile 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 Classic Mobile 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

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile configurations:

- "View Setup and Configuration"

To create, change, or delete Salesforce Classic Mobile data sets:

- "Manage Mobile Configurations"

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 Classic Mobile

Configuring Salesforce Classic Mobile 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 Classic Mobile app.

Tips for setting up Salesforce Classic Mobile access for partner users:

- Before setting up Salesforce Classic Mobile for partner users, you must configure partner user accounts and purchase mobile licenses for each partner portal user that will be using Salesforce Classic Mobile. Partner user profiles must be assigned to at least one active partner portal before partner users can use Salesforce Classic Mobile. If a user profile is assigned to multiple partner portals, only the first assigned partner portal will be accessible using Salesforce Classic Mobile.
- Custom mobile list views don't affect list views in the partner portal.
- If you make User data sets available in the Salesforce Classic Mobile 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 Classic Mobile

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile configurations, data sets, mobile devices, and users:

- "View Setup and Configuration"

To create, change, or delete Salesforce Classic Mobile 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 Classic Mobile

To improve the integration between the Salesforce Classic Mobile 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 Classic Mobile 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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To create or change custom buttons or links:
- "Customize Application"

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.
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 Classic Mobile

Notifying Users about Salesforce Classic Mobile Availability

When you're ready to deploy the Salesforce Classic Mobile 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 and BlackBerry users, the download URL is `mobile.salesforce.com`. The link is the same for the initial download and for subsequent upgrades.
- If you manage BlackBerry devices with a BlackBerry Enterprise Server, you can use Application Push to remotely deliver Salesforce Classic Mobile to users. For more information about BlackBerry Enterprise Application Push, see the *Salesforce Classic Mobile Implementation Guide*.
- You can obtain the iPhone download URL from iTunes. Open iTunes, click **iTunes Store**, then search for Salesforce Classic Mobile. 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 Classic Mobile**. 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 Classic Mobile users from Salesforce:

1. Create an email template that informs users about the availability of Salesforce Classic Mobile. 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 Classic Mobile users only.

   Note: The `Mobile User` checkbox on the user record assigns a mobile license to users, which enables use of the full version of Salesforce Classic Mobile. But other Salesforce users can access the free version of Salesforce Classic Mobile without an assigned mobile license, so you can't filter for all Salesforce Classic Mobile users by license. Create a view for users of the free version by filtering by roles or profiles instead.
3. Send mass email to your Salesforce Classic Mobile users, using the custom view that you created. From Setup, enter *`Mass Email Users`* in the `Quick Find` box, then select **Mass Email Users**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To create HTML email templates:
- "Edit HTML Templates"

To send mass emails to users:
- "Mass Email"

  AND

  "Manage Users"

SEE ALSO:

Setting Up Salesforce Classic Mobile

Salesforce Classic Mobile FAQ for Administrators

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

Is the Salesforce Classic Mobile mobile app secure?

All data transmitted between Salesforce and Salesforce Classic Mobile 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.

My Salesforce Classic Mobile users have Android, BlackBerry, and iPhone devices. Can we have multiple types of device in one organization?

Yes, one organization can have multiple types of devices. However, a Salesforce Classic Mobile user can only have one active device.

Is there an easy way to deploy Salesforce Classic Mobile to all of my BlackBerry users?

If your organization manages BlackBerry smartphones using the BlackBerry Enterprise Server (BES), you can use Application Push. Application Push is an administrator-initiated delivery technology on the BlackBerry Enterprise Server that installs applications on BlackBerry smartphones remotely. This technology is not developed or supported by Salesforce, but BlackBerry Enterprise Server administrators can use it to install Salesforce Classic Mobile on their BlackBerry users' mobile devices.

For instructions on how to configure the BlackBerry Enterprise Server v4.1 to push Salesforce Classic Mobile to your BlackBerry users, see "BlackBerry Enterprise Server Application Push" in the *Salesforce Classic Mobile Implementation Guide*.

You can find detailed information about Application Push in the official *BlackBerry Enterprise Server Administrator Guide* from Research in Motion in the sections "Making additional BlackBerry device software and applications available to users" and "Creating software configurations." If you have any technical issues with Application Push, contact Research in Motion Support.

Manage Salesforce Classic Mobile Configurations

To manage your Salesforce Classic Mobile 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:

Salesforce Classic Mobile Overview for Administrators

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile configurations:

- "View Setup and Configuration"

To create, change, or delete Salesforce Classic Mobile configurations:

- "Manage Mobile Configurations"

Salesforce Classic Mobile Permissions

A mobile license is required for each user who will access the full version of the Salesforce Classic Mobile 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 the full version of Salesforce Classic Mobile on their mobile devices before you're ready to deploy the app, disable the `Mobile User` checkbox for all your users.

Any Salesforce user who doesn't have a mobile license can download a free, restricted version of Salesforce Classic Mobile. Starting with Summer '13, the free version of Salesforce Classic Mobile is disabled by default in all new organizations. You can enable it to give users access to Salesforce on their mobile devices.

To enable the free version of Salesforce Classic Mobile:

1. From Setup, enter *`Salesforce Classic Settings`* in the `Quick Find` box, then select **Salesforce Classic Settings**.
2. Click **Edit**.
3. Select `Enable Mobile Lite`.
4. Click **Save**.

SEE ALSO:

Salesforce Classic Mobile Overview for Administrators

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile configurations:

- "View Setup and Configuration"

To create, change, or delete Salesforce Classic Mobile configurations:

- "Manage Mobile Configurations"

Manage Salesforce Classic Mobile Tabs

To manage the tabs for a Salesforce Classic Mobile 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:

Salesforce Classic Mobile Overview for Administrators

Manage Salesforce Classic Mobile Configurations

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile configurations:

- "View Setup and Configuration"

To manage Salesforce Classic Mobile tabs:

- "Manage Mobile Configurations"

Manage Salesforce Classic Mobile Views

To manage the custom views for a Salesforce Classic Mobile 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:

Salesforce Classic Mobile Overview for Administrators

Manage Salesforce Classic Mobile Configurations

Manage Salesforce Classic Mobile Devices

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile devices and users:

- "View Setup and Configuration"

To manage Salesforce Classic Mobile custom views:

- "Manage Mobile Configurations"

Salesforce Classic Mobile Usage Data in Custom Report Types

You can create custom report types with data that shows how your organization uses Salesforce Classic Mobile. For example, the reports can show how often users access Salesforce Classic Mobile, which mobile device models they use, and so forth.

To create a custom report type with Salesforce Classic Mobile 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 Classic Mobile-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 (PIN for BlackBerry or UDID for iOS)
Device Application Version	Installed version of Salesforce Classic Mobile
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

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

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 Classic Mobile after 20 minutes of inactivity in the app or on the device in general.
- Mobile session reports only have usage data for the Salesforce Classic Mobile app and not other Salesforce mobile apps, such as the Salesforce1 apps.
- Some devices do not provide every physical attribute. For example, Apple devices do not provide brand.

Manage Salesforce Classic Mobile Devices

After a user installs the Salesforce Classic Mobile 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 Classic Mobile.
- 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 Classic Mobile app to evaluate the effectiveness of your organization's Salesforce Classic Mobile 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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile devices and users:
- "View Setup and Configuration"

To manage Salesforce Classic Mobile devices:
- "Manage Mobile Configurations"

IN THIS SECTION:

Permanently Link Salesforce Classic Mobile 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 Classic Mobile activation.

Viewing Salesforce Classic Mobile Device Information

Set Salesforce Classic Mobile Session Timeout Values

Erasing Data in Salesforce Classic Mobile

Deleting Mobile Devices

SEE ALSO:

Salesforce Classic Mobile Overview for Administrators

Manage Salesforce Classic Mobile Configurations

Permanently Link Salesforce Classic Mobile 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 Classic Mobile 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 Classic Mobile app.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile settings:

- "View Setup and Configuration"

To change Salesforce Classic Mobile settings:

- "Manage Mobile Configurations"

Viewing Salesforce Classic Mobile Device Information

Salesforce collects information about a mobile user's device the first time the user logs in to the Salesforce Classic Mobile 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

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view Salesforce Classic Mobile devices and users:
- "View Setup and Configuration"

To manage Salesforce Classic Mobile 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, BlackBerry, 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 Classic Mobile 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 Classic Mobile Session Timeout Values

For security reasons, the Salesforce Classic Mobile 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 Classic Mobile timeout setting if a mobile device's operating system has its own locking mechanism.

To change the Salesforce Classic Mobile 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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To set Salesforce Classic Mobile session timeout values:

- "Manage Mobile Configurations"

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 Classic Mobile 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 Classic Mobile server prevented the message from being sent. Try again later.

Result	Description
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 Classic Mobile

When a user accesses the Salesforce Classic Mobile 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 Classic Mobile 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 Classic Mobile 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.

SEE ALSO:

Manage Salesforce Classic Mobile Devices

Deleting Mobile Devices

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To delete the Salesforce data on a device running Salesforce Classic Mobile:

- "Manage Mobile Configurations"

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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Free version available in: **All** editions except **Database.com**

Full version available in: **Performance**, **Unlimited**, and **Developer** Editions, and for an extra cost in: **Professional** and **Enterprise** Editions

USER PERMISSIONS

To view mobile devices and users:
- "View Setup and Configuration"

To delete mobile devices:
- "Manage Mobile Configurations"

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.
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 Classic Mobile

Salesforce Classic Mobile App Limits

Mobile Device Limits

BlackBerry smartphones	• Mobile users running versions 4.0 - 4.3 of the BlackBerry operating system can still download and install the Salesforce Classic Mobile app; however, the mobile server will detect the older operating system and send version 11.6 of Salesforce Classic Mobile, which was the last release that supported BlackBerry operating system versions 4.0 - 4.3. Users on version 11.6 of Salesforce Classic Mobile can't use any of the new features included in the current release or future releases. • BlackBerry touchscreen devices use the same Salesforce Classic Mobile app as other BlackBerry devices, so some aspects of Salesforce Classic Mobile aren't optimized for the touchscreen interface.
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 Classic Mobile for the iPhone and iPod touch devices, or delete the Salesforce Classic Mobile 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 Classic Mobile for iPhone product. Additional limitations are described in the Order Form Supplement for Salesforce Classic Mobile for iPhone, which users are required to accept upon download or installation of the Salesforce Classic Mobile for iPhone product.

Dashboards Limits

When working with dashboards in Salesforce Classic Mobile, these limitations exist:

- You can't create or edit dashboards.
- Links to custom report details are disabled.
- The minimum BlackBerry operating system requirement for mobile dashboards is 4.5. Mobile dashboards are compatible with version 4.2 and 4.3, but tables in the dashboards might not display properly. To find out which operating system is installed on your BlackBerry smartphone, go to the BlackBerry home screen, and then select **Options** > **About**.

Chatter Mobile for BlackBerry

Configure Chatter Mobile for BlackBerry

Important: As of Summer '14, the Chatter Mobile for BlackBerry app is no longer supported. You can continue to use the app, but Salesforce no longer provides support in the form of bug fixes or enhancements for any issues you may encounter. Talk to your Salesforce administrator about migrating to the Salesforce1 app, the new Salesforce mobile experience.

Chatter Mobile for BlackBerry is built as a connected app. A connected app is an application that integrates with Salesforce using APIs. Connected apps allow administrators to set various security policies and have explicit control over who may use the applications. Administrators can view and manage the Chatter Mobile for BlackBerry settings in the same way they view and manage other connected app settings.

Chatter Mobile for BlackBerry is automatically installed as part of a managed Salesforce connected apps package when one of these events occurs:

- A user in your organization downloads the Chatter Mobile for BlackBerry mobile app and authenticates with your organization by logging in to the mobile app.
- An existing Chatter Mobile user's session refreshes.

  Note: Sessions refresh automatically between every 15 minutes and 12 hours while a user is in the app based upon the session `Timeout value` set for your organization; this is often undetected by the user.

Alternatively, an administrator can manually install the Salesforce1 and Chatter Apps connected apps package to view and manage the settings before the package is automatically installed.

The connected apps package includes a separate connected app for the BlackBerry mobile device type.

Important: Unless an administrator manually installs the package, you'll only see the Chatter Mobile for BlackBerry connected app after someone in your organization activates a mobile app or an existing user's session refreshes.

Administrators can use profiles, permission sets, and IP range restrictions to control which users can access the app. These settings are controlled on the Chatter Mobile for BlackBerry connected app detail page, which you can access from Setup by entering *`Connected Apps`* in the `Quick Find` box, then selecting the option for managing connected apps.

The app displays an error message if a restricted user tries to open it.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To edit your mobile app settings:
- "Customize Application"

To view your mobile app settings:
- "View Setup and Configuration"

Mobile Dashboards for iPad

Let Users View Dashboards on the iPad

The Mobile Dashboards for iPad app is automatically enabled for your organization so your users can access the app without any configuration on your part.

Important: As of Summer '15, the Mobile Dashboards for iPad app is no longer supported. You can continue to use the app, but Salesforce no longer provides support in the form of bug fixes or enhancements for any issues you may encounter. Talk to your Salesforce administrator about migrating to the Salesforce1 app, the new Salesforce mobile experience.

You can disable the app if you don't want users accessing Salesforce data from mobile devices and you can easily re-enable it if you change your mind later.

To configure access to Mobile Dashboards for iPad:

1. From Setup, enter *Mobile Dashboards* in the Quick Find box, then select **Mobile Dashboard Settings**.
2. Select or deselect Enable the Mobile Dashboards iPad app for all users.
3. Click **Save**.

Users can download and install the Mobile Dashboards for iPad app from the Apple App Store or AppExchange Mobile.

Aside from editions noted, the app is available to organizations enabled with REST API.

EDITIONS

Available in: Salesforce Classic

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

USER PERMISSIONS

To view Mobile Dashboards for iPad settings:

- "View Setup and Configuration"

To modify Mobile Dashboards for iPad settings:

- "Customize Application"

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"

Install Packages and Manage Apps

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: **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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **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," "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

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 816.

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 809.
- 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 801.

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.

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.

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"

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

Limitations and Considerations for Platform Encryption

Uninstalling a Package

You can remove any installed package, including all of its components and all data in the package. Additionally, 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, as well as any associated notes and 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 period of 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 809.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

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

USER PERMISSIONS

To uninstall packages:
- "Download AppExchange Packages"

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, as well as 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.

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.

After an uninstall, Salesforce automatically creates an export file containing the package data, as well as any associated notes and 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 period of 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.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **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"

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: **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**
`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.

Attribute	Description
`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
`API Access`	The type of access that the API and dynamic Apex code that package components have. The default setting is **Unrestricted**, which means that all package components that access the API have the same access as the user who is logged in. Click **Enable Restrictions** or **Disable Restrictions** to change the API and dynamic Apex access permissions for a package.
`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`.

Attribute	Description
`Version Number`	The version number for the latest installed package version. The format is *majorNumber.minorNumber.patchNumber*, 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: **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:

Assigning Licenses for Managed Packages

Assigning Licenses for Installed Packages

Removing Licenses for Installed Packages

Responding to License Manager Requests

Assigning 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 will not appear on this list, as you cannot assign licenses for them.

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 will not 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

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"

Assigning Licenses for Installed Packages

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.

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"

SEE ALSO:

Managing Licenses for Installed Packages

Removing Licenses for Installed Packages

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**.

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"

You can also remove licenses for an AppExchange package from a single user using the following options:

1. From Setup, enter *Users* in the Quick Find box, then select **Users** and click **Remove** next to the package in the managed packages list.

2. From Setup, enter *Installed Packages* in the Quick Find box, then select **Installed Packages**. Then, click **Manage Licenses** next to the package name, and click **Remove** next to the user.

SEE ALSO:

Managing Licenses for Installed Packages

Responding to License Manager Requests

A license manager is a Salesforce 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

EDITIONS

Available in: Salesforce Classic

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"

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.

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"

For details of the PackageLicense and UserPackageLicense objects and a code sample, see the Object Reference for Salesforce and Force.com.

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?
- Why did my uninstall fail?
- 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

Available in: **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

Why did my uninstall fail?

Salesforce prevents you from uninstalling a package if it causes any remaining components to malfunction.

SEE ALSO:

Uninstalling a Package

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.

However, unmanaged packages can also have a namespace prefix if they originated from an organization that contained a managed package. When you install an unmanaged package that contains a namespace prefix, Salesforce replaces the developer's namespace prefix with yours.

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.

Printable Resources for Administrators

In addition to online help, Salesforce publishes printable documentation to help you successfully administer Salesforce.

These documents include tip sheets, user guides, implementation guides, and other resources that describe the features and capabilities of Salesforce. These documents are available as Adobe® PDF files. Adobe Reader® is required to open PDF files; to download the latest version of Reader, go to `www.adobe.com/products/acrobat/readstep2.html`.

Salesforce Implementations

- *Salesforce Enterprise Edition Upgrade Guide*
- *Setting Up Salesforce Group Edition*
- *Salesforce Limits Quick Reference Guide*

Security and Data Management

- *Security Implementation Guide*
- *Managing Duplicate Records in Salesforce*
- *Single Sign-On Implementation Guide*
- *Platform Encryption Implementation Guide*
- *Understanding User Sharing*
- *Understanding Defer Sharing Calculations*

- *Managing Data Quality*
- *Importing Your Organization's Accounts and Contacts*
- *Using Mass Delete to Undo Imports*
- *Getting Started with Divisions*
- *Data Loader Guide*
- *Salesforce Field Reference Guide*
- *Resolving Data Conflicts and Errors in Force.com Flex Apps*
- *Salesforce Identity Implementation Guide*
- *Identity Connect Implementation Guide*

Mobile Administration

- *Salesforce1 Mobile App Admin Guide*
- *Salesforce Classic Mobile Implementation Guide*

Videos for Salesforce Administrators

In addition to online help, Salesforce creates video demos to help you learn about our features and successfully set up and manage Salesforce.

Data Import

Video Title	For End Users	For Admins
Cleaning Up Your Import File Learn how to clean up your import files and get Salesforce ready, and best practices for keeping data clean once it's been imported.		✔
Cleaning and Preparing Your Data Using Excel Excel offers many features and functions to make quick work of getting your data files ready for import. We show you some practical ways to use these features with your import data.		✔
Choosing the Right Tool Learn Data Loader in depth, so you can decide whether it's right for your needs. We compare it to the Import Wizards and also list some other tools to consider.		✔
Owner IDs and Parent IDs Learn, step by step, which objects you should import, and when. We cover how to make sure each child object, such as opportunities, has the correct owner and parent record, and we show you a demo in the user interface of how to do this using the Data Loader tool.		✔
Best Practices for Importing Data		✔

Video Title	For End Users	For Admins
Learn the top pain points experienced by our customers, so you can avoid them entirely! This video details how to delete a bad import, how to back up data before import, and more.		
Importing Your Accounts and Contacts—Part 1: Exporting Your Data In this video, we walk you through how to import Account and Contact data using the Data Import Wizard. Once you have your data in a csv file, you can use the wizard to import it and map fields.		✓
Importing Your Accounts and Contacts—Part 2: Importing Your Data		✓

Users' Access to Data

Video Title	For End Users	For Admins
Who Sees What: Overview Learn how you can control who sees what data in your organization.		✓
Who Sees What: Organization Access Learn how to restrict login through IP ranges and login hours.		✓
Who Sees What: Object Access Learn how you can grant users access to objects by using profiles.		✓
Who Sees What: Organization-Wide Defaults Learn how you can restrict access to records owned by other users.		✓
Who Sees What: Record Access via the Role Hierarchy Learn how you can open up access to records using the role hierarchy.		✓
Who Sees What: Record Access via Sharing Rules Learn how you can grant access to records using sharing rules.		✓
Who Sees What: Field-level Security Learn how you can restrict access to specific fields on a profile by profile basis.		✓
Who Sees Whom: User Sharing Learn how you can control visibility among users in your organization.		✓
Creating a Criteria-Based Sharing Rule Learn how to create a sharing rule based on a field value in a record.		✓
Who Sees What: Permission Sets		✓

Video Title	For End Users	For Admins
Learn how to give users more permissions and access settings without changing profiles.		

Managing Users

Video Title	For End Users	For Admins
Removing Users' Access to Salesforce Deactivating users in Salesforce removes access to their account data while preserving their historical activity and records. Once you understand why you deactivate users rather than deleting them, learn how to deactivate someone and see what happens to their data.		✔

INDEX

A

B

C

D

E

F

G

H

I

M

N

O

P

T

U

V

W