Salesforce Identity connects your Salesforce org users with external apps and services while providing administrative tools for monitoring, maintaining, and reporting user apps and user authorization.

Salesforce Identity is an identity and access management (IAM) service with the following features.

- Cloud-based user directories, so user accounts and information are stored and maintained in one place, while available to other services or apps.
- Authentication services to verify users and keep granular control over user access. You can require two-factor authentication, select which apps users can use, and set how often individual users log in to maintain their session.
- Access management and authorization for third-party apps, including UI integration, so a user’s apps and services are readily available.
- App user provisioning, which streamlines the process for providing and removing access to apps to multiple users simultaneously.
- An API for viewing and managing Identity features.
- Identity event logs for creating reports and dashboards on single sign-on (SSO) and connected app usage.
- Salesforce Identity Connect for integrating Microsoft Active Directory (AD) with Salesforce. Identity Connect allows you to manage AD users and Salesforce users simultaneously. You can configure Identity Connect to give AD users access to their Salesforce orgs without logging in again.

To implement Salesforce Identity, use any of the following.

**Security Assertion Markup Language (SAML)**

Security Assertion Markup Language (SAML) is an XML-based protocol that allows you to transfer user information between services, for example, from Salesforce to Microsoft 365. Apps use this information to authorize users and enable SSO. Salesforce supports SAML for SSO into Salesforce from a corporate portal or identity provider.

**OAuth 2.0**

OAuth 2.0 is an open protocol used to allow secure authorization between apps. OAuth authorization flows describe the options for implementing OAuth in Salesforce orgs. For more information on specific flows, see REST API Developer Guide.

**OpenID Connect**

OpenID Connect is an authentication protocol based on OAuth 2.0 that sends identity information between services. With OpenID Connect, users can log in to another service, like Gmail, and then access their Salesforce org without logging in again.

**My Domain**

My Domain allows you to define your own domain name within the Salesforce domain (for example, https://companyname.my.salesforce.com). My Domain makes it easier to manage login and authentication and allows you to customize your login page. Salesforce requires My Domain if you want to use some features, including Lightning components in Lightning tabs, Lightning pages, or as a standalone app.

**Connected Apps**

A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect. Connected apps use these protocols to authenticate, authorize, and provide SSO for external apps. The external apps that are integrated with Salesforce can run on the customer success platform, other platforms, devices, or SaaS subscriptions.
What Is Salesforce Identity?

App Launcher
The App Launcher gives your users easy access to apps that they use most often. Users go to the App Launcher to launch Salesforce, on-premises, and connected (third-party) apps without logging in again (referred to as single sign-on). The App Launcher displays tiles that link to the available apps. It is available to all Lightning Experience users. Salesforce Classic users must have the Use Identity Features permission to get the App Launcher.

Identity License
The Identity license grants users access to Identity features. Salesforce Identity connects Salesforce users with external applications and services, while giving admins control over authentication and authorization for these users.

Identity licenses are included with all paid user licenses in Enterprise, Performance, and Unlimited Editions. Ten free Identity user licenses are included with each new Developer Edition org. You can also purchase a standalone Identity-only license.

External Identity License
An External Identity license lets you deliver identity services, including (SSO) to external users. It is a standalone license that you can buy for blocks of users who are consumers of your business, such as customers, purchasers, patients, partners, and dealers.

The license is included with all paid user licenses in Enterprise, Performance, and Unlimited Editions. Ten free External Identity user licenses are included with each new Developer Edition org.

Identity Provider and Service Provider integration
An identity provider is a trusted provider that lets you use single sign-on (SSO) to access other websites. A service provider is a website that hosts apps. You can enable Salesforce as an identity provider and define one or more service providers. Your users can then access other apps directly from Salesforce using SSO. SSO is a great help to your users—instead of having to remember many passwords, they only have to remember one.

Salesforce Identity Connect
Identity Connect integrates Microsoft Active Directory (AD) with Salesforce. User information entered in AD is shared with Salesforce seamlessly and instantaneously. Companies that use AD for user management can use Identity Connect to manage Salesforce accounts.

Two-Factor Authentication
Two-factor authentication is the most effective way to protect your org’s user accounts. When two-factor authentication is enabled, users are required to log in with two pieces of information, such as a username and a one-time password (OTP). Admins enable two-factor authentication through permissions or profile settings. Users register for two-factor authentication through their own personal settings. They can use an OTP generator app, such as Salesforce Authenticator or Google Authenticator. Or they can use hardware devices, such as U2F security keys. With two-factor authentication enabled, users are required to log in with two pieces of information, such as a username and a one-time password (OTP). Salesforce supports user-defined OTPs and OTPs generated from software or hardware devices.
CHAPTER 2  How to Use Identity

Using a combination of Salesforce Identity features, you can make it easy for employees to access Salesforce. You can also have more control over which users access which third-party apps.

Salesforce Identity provides single sign-on (SSO) for employees to sign in to multiple Salesforce and third-party apps.

Here’s an example of how the company Universal Containers uses several Salesforce Identities features to meet its login requirements.

**Example:** Universal Containers has employees that sign in to multiple apps to get their job done. To make it easier for employees to log in, the company wants an SSO solution and decides to use Salesforce Identity to implement it. To use Salesforce as an SSO provider (also called the identity provider), Universal Containers must set up a subdomain using My Domain. Then the company creates and manages authorization settings to control how employees log in to the subdomain.

Universal Containers uses the Security Assertion Markup Language (SAML) protocol to pass authentication and authorization information between its subdomain and other providers. Users logged in to the Universal Containers subdomain can use third-party apps without logging in again. Likewise, Universal Containers can give users access to its subdomain from approved third-party apps without logging in again. In this case, the third-party app is the identity provider. SSO is available between any app that supports SAML standards, such as G Suite.

Universal Containers decides to enhance security while enabling SSO. The company implements two-factor authentication to require that users enter a unique one-time code when they log in. Universal Containers can also customize the login page to reflect its corporate identity. This way, when users log in, they can see where they are before entering authentication information.

Using the App Launcher, Universal Containers controls which apps are available to individual users and how long users can access Salesforce before reauthenticating. The App Launcher is also used to extend SSO to mobile users.

For login and user management, Universal Containers uses Active Directory (AD). The company decides to integrate AD with Salesforce using Identity Connect. With Identity Connect, admins can manage Salesforce users through the corporate AD database. Then users can log in to Salesforce using their AD credentials. And changes to users in Active Directory are immediately updated in Salesforce.

Universal Containers has an external identity community. They use the dynamic branding feature, where branding changes at run time according to who logs in and from where. Universal Containers displays different logos depending on whether the user is an employee, customer, partner, or guest. Branding impacts the entire login experience—the login page, plus any secondary pages that support 2FA, Terms & Conditions, or login flows.

After the system is up and running, Universal Containers builds reports and dashboards to track user login history and app usage. With these reports, Salesforce admins can adjust authorization as needed.
CHAPTER 3  My Domain

In this chapter ...

- Set Up a My Domain Subdomain
- My Domain URL Changes
- Add Identity Providers to the My Domain Login Page
- Create an Interview-Based Login Page with My Domain Discovery
- Best Practices for Implementing My Domain
- Get System Performance and Maintenance Information with My Domain

Create your own subdomain for your Salesforce org to better manage login and authentication. With a subdomain, you can include your company name in your URL, such as https://yourcompanyname.my.salesforce.com. You can also customize your login page, such as add your logo, change the color scheme, or add your own content on the right side of the login page. To create your own subdomain, you use the Salesforce Identity My Domain feature.

To get an overview and learn about the benefits of My Domain, watch Set Up My Domain.

With My Domain, you create a subdomain within the salesforce.com domain. For example, trailhead is a subdomain of the Salesforce domain: trailhead.salesforce.com. With a subdomain, you replace the instance URL that Salesforce assigned you, like https://na30.salesforce.com, with your chosen domain name, like https://somethingcool.my.salesforce.com.

With a My Domain subdomain, you can:
- Highlight your business identity with your unique domain URL
- Brand your login page and customize content on the right side of the page
- Block or redirect page requests that don’t use the new domain name
- Work in multiple Salesforce orgs at the same time
- Set custom login policy to determine how users are authenticated
- Let users log in using a social account, like Google and Facebook, from the login page
- Allow users to log in once to access external services

My Domain is required to use many Salesforce features, including:
- Single sign-on (SSO) with external identity providers
- Social sign-on with authentication providers, such as Google and Facebook
- Lightning components in Lightning component tabs, Lightning pages, the Lightning App Builder, or standalone apps

My Domain is available for sandbox environments.

Your My Domain subdomain uses standard URL format:
- Protocol: https://
- Subdomain prefix: your brand or term
- Domain: my.salesforce.com

Your name can include up to 34 letters, numbers, and hyphens. You can’t start the name with root, status, or a hyphen.

When you create a subdomain with My Domain, Salesforce is enabled as the identity provider. After you deploy your subdomain, you can change identity providers. You can also increase security for your org by customizing your domain’s login policy.
The best way to learn is by doing. Before you continue, go to Trailhead to learn about My Domain, Customize your Login Process with My Domain.
Set Up a My Domain Subdomain

Implementing your subdomain with My Domain is quick and easy.

1. **Find a domain name that’s available and register for it.**
2. **Test your domain name and deploy it to your entire org.**
3. **Set the login policy for users accessing your pages.**
4. **Customize the logo, background, and right-frame content of your login page.**
5. **Add or change the identity providers available on your login page.**
6. **Set up My Domain with Login Discovery to let users log in with only an identifier, instead of a username and password.**
7. **Rename your My Domain subdomain if your company name or branding changes.**

IN THIS SECTION:

1. **Define Your My Domain Subdomain Name**
   To set up a My Domain subdomain, you choose a name for your subdomain and register it with Salesforce domain registries worldwide. You can try out names and check availability before registering it.

2. **Test and Deploy Your New My Domain Subdomain**
   After you set up your subdomain with My Domain, test it and then roll it out to your users. Testing gives you the chance to explore your subdomain. It also helps you verify URLs for pages before deploying your subdomain to your users. Make sure that you thoroughly test all customizations, such as custom buttons and Visualforce pages.

3. **Set the My Domain Login Policy**
   Manage your user logins by customizing the login policy for your My Domain subdomain. By default, users log in from a generic Salesforce login page, bypassing the login page specific to your subdomain. To disable authentication for users who don’t use your subdomain login page, set a login policy. If you don’t set a login policy, users can make page requests without your subdomain name, such as when using old bookmarks.

4. **Customize Your My Domain Login Page with Your Brand**
   My Domain gives you a point-and-click way to brand the page that prompts users to log in to your Salesforce org. You can replace the Salesforce logo with yours and change your background and login button colors. You can also display content to the right of your login form. Branding options apply to the entire login experience, including pages for users to verify their identity and reset passwords. They also apply to login flows.
Define Your My Domain Subdomain Name

To set up a My Domain subdomain, you choose a name for your subdomain and register it with Salesforce domain registries worldwide. You can try out names and check availability before registering it.

Choose a name that’s unique and meaningful, like your company name, which would make the URL https://companyname.my.salesforce.com, or something more specific within your company, like https://companyEU.my.salesforce.com. You can rename your My Domain subdomain in production orgs. But you can’t rename a sandbox, developer, or trial org subdomain.

1. From Setup, enter My Domain in the Quick Find box, then select My Domain.
2. Enter the name that you want to use for your My Domain subdomain. Your name can include up to 34 letters, numbers, and hyphens.

Salesforce adds the rest of the domain name. If you’re creating the subdomain in a developer org, the domain name is -dev-ed.my.salesforce.com. Your production org has the my.salesforce.com suffix.

**Important:** Avoid entering personal information in your domain name. Instead, enter only public information.

3. Click Check Availability. If your name is already taken, choose a different one.
4. Click Register Domain.
5. You receive an email when your subdomain name is ready for testing. It can take a few minutes.

Before making your new My Domain subdomain available to your users, test that your org’s URLs work with your new subdomain name. Then you can roll it out to your users.

Test and Deploy Your New My Domain Subdomain

After you set up your subdomain with My Domain, test it and then roll it out to your users. Testing gives you the chance to explore your subdomain. It also helps you verify URLs for pages before deploying your subdomain to your users. Make sure that you thoroughly test all customizations, such as custom buttons and Visualforce pages.

**Suggestions for Deploying a My Domain**

- Communicate the upcoming change to your users before deploying it.
- Deploy your new subdomain when your org receives minimal traffic, like during a weekend, so that you can troubleshoot while traffic is low.
- Make sure you update all application URLs before deploying a My Domain subdomain. For example, the Email Notification URL option in Chatter Answers continues to send notifications with the old URLs to internal users unless you update it.

**Note:** If your My Domain subdomain is registered but not deployed, URLs contain your subdomain name when you log in from the My Domain login page. However, links that originate from merge fields that are embedded in emails sent asynchronously, such as workflow emails, still use the old URLs. After your domain is deployed, those links show the new My Domain URLs.
1. Return to the My Domain Setup page using one of these ways. Click the login link in the activation email that you received. Or, from Setup, enter *My Domain* in the Quick Find box, then select *My Domain*. Or, log out of your org, and log in to Salesforce using your new My Domain subdomain name.

2. Test the new subdomain by clicking tabs and links. In the browser address bar, notice that the URLs to all your pages display your new subdomain.

   If you’ve customized your org, for example, with buttons or Visualforce pages, make sure that you test your changes thoroughly. Look for broken links due to hard-coded references (instance-based URLs such as `https://na30.salesforce.com`). Change these URLs to use your subdomain instead. For more information, search for “hard-coded references” in *Salesforce Help*. Test them in a sandbox environment first.

3. Optionally, test the subdomain in a sandbox environment.

4. Optionally, customize your subdomain login page, and add authentication services, like single sign-on.

   While you can make these changes after you deploy, it's better to set up and test them in a smaller environment.

5. To roll out the new My Domain subdomain to your org, from Setup, enter *My Domain* in the Quick Find box, then select *My Domain*. Click *Deploy to Users*, and click *OK*.

   This step is often overlooked and causes much confusion. Your users can’t access the org with the subdomain URLs until you deploy it.

   When you deploy your My Domain subdomain, it’s activated immediately. You can now set login policies in the Domain Settings section that appears after you deploy your domain. See Set the My Domain Login Policy.

   Help your users get started using your new subdomain by providing links to pages they use frequently, such as your login page. Let your users know if you changed the login policy, and encourage them to update their bookmarks the first time they’re redirected.

---

**Set the My Domain Login Policy**

Manage your user logins by customizing the login policy for your My Domain subdomain. By default, users log in from a generic Salesforce login page, bypassing the login page specific to your subdomain. To disable authentication for users who don’t use your subdomain login page, set a login policy. If you don’t set a login policy, users can make page requests without your subdomain 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. Choose a redirect policy.

   a. To allow users to continue using URLs that don’t include your subdomain name, select *Redirect to the same page within the domain*.

   ```
   Note: Bookmarks don’t work when *Redirect to the same page within the domain* is selected for partner portals. Manually change the existing bookmarks to point to the new subdomain URL by replacing the Salesforce instance name with your My Domain subdomain name. For example, replace `https://na30.salesforce.com/` with `https://yourDomain.my.salesforce.com/` in the bookmark’s URL.
   ```

   b. To remind users to use your My Domain subdomain name, select *Redirected with a warning to the same page within the domain*. After reading the warning, users are redirected to the page. Select this option for a few days or weeks to help users transition to a new domain name.

   c. To require users to use your subdomain name when viewing your pages, select *Not redirected*.
4. Click Save.

**Customize Your My Domain Login Page with Your Brand**

My Domain gives you a point-and-click way to brand the page that prompts users to log in to your Salesforce org. You can replace the Salesforce logo with yours and change your background and login button colors. You can also display content to the right of your login form. Branding options apply to the entire login experience, including pages for users to verify their identity and reset passwords. They also apply to login flows.

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, click *Choose File* and upload an image file.
   - Images can be .jpg, .gif, or .png files up to 100 KB. The maximum image size is 250 px by 125 px.
4. To customize your login page background, click ![ ] and choose your hexadecimal color code.
5. To display content in the right frame URL, enter a URL.
   - By default, the right side displays the current Salesforce promotions, `https://c.salesforce.com/login-messages/promos.html` in an iframe.
   - The iframe creates an inline frame, which embeds an HTML document into the current page.
   - You can show your own content by supplying a URL that uses SSL encryption and the `https://` prefix. The iframe dynamically expands to fill about 50% of the page. To build your own custom iframe using responsive web design, use the *My Domain Sample* template.
   - For an example of a right-frame URL, go to `https://sfdclogin.herokuapp.com/news.jsp`.
6. Click *Save*.

**My Domain URL Changes**

When you set up a subdomain for your org with My Domain, all your application URLs, including Visualforce pages, also change. Make sure you that update all application URLs before deploying a My Domain subdomain. For example, the Email Notification URL option in Chatter Answers continues to send notifications with the old URLs to internal users unless you update it. This table compares URLs before and after setting up a subdomain.

<table>
<thead>
<tr>
<th>URL Type</th>
<th>Old URL</th>
<th>New URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application page or tab</td>
<td><code>https://&lt;instance&gt;.salesforce.com/&lt;pageID&gt;</code></td>
<td><code>https://&lt;subdomain&gt;.my.salesforce.com/&lt;pageID&gt;</code></td>
</tr>
</tbody>
</table>

**Note:** If you implement My Domain in a sandbox environment, the URL format is `https://<subdomain>--<sandboxname>.my.salesforce.com`. 
### Add Identity Providers to the My Domain Login Page

Allow users to authenticate using alternate identity provider options directly from your My Domain login page. If you’ve enabled single sign-on (SSO) and configured SAML, or set up external authentication providers, you can display them on the login page. Users are sent to the identity provider’s login screen to authenticate and then redirected back to Salesforce.

Available authentication services include all providers configured as SAML SSO identify providers or external authentication providers, except Janrain. You can’t use Janrain for authentication from the login page.

**Note:** Authentication configuration settings show up only after you deploy My Domain.

1. From Setup, enter *My Domain* in the Quick Find box, then select *My Domain*.
2. Under Authentication Configuration, click *Edit*.
3. Select the authentication services you want to make available on the login page.
4. Click *Save*.

You can list all your org’s available SSO identity providers on your login page. If you have several, consider setting up your login page with the Login Discovery page type. For details, see Create an Interview-Based Login Page with My Domain Login Discovery in Salesforce Help.

### Create an Interview-Based Login Page with My Domain Login Discovery

Configure My Domain with Login Discovery to simplify the login process for users. Login Discovery is sometimes called interview-based login because it’s a two-step process. First, users identify themselves with an email address or phone number at the login page. Next, users verify themselves depending on the identifier entered. Users can verify themselves with a password, their SSO credentials, or Lightning Login. You set up Login Discovery from the My Domain Setup page after you create an Apex class that implements the `MyDomainLoginDiscoveryHandler` interface.

My Domain Login Discovery requires that My Domain is set up for your org. If you’ve already set up My Domain, you can migrate users to the Login Discovery login process.

Login Discovery eliminates the onerous task of managing forgotten usernames. With Login Discovery, your users can log in with something they are likely to remember, like their email address or phone number. Also, if your org is configured with multiple identity providers (IdP) for SSO, Login Discovery can direct users to the suitable IdP. If your login page contains an SSO button along with the username and password fields, users might not notice the SSO button or know what it’s for. If you’re using Login Discovery, no decisions are required.

Login Discovery is helpful when you have different login processes depending on the situation, such location or device type. For example, you might have separate IdPs for mobile and desktop.
users. Instead of having a login page with buttons for both, Login Discovery determines where users are logging in from and directs them to the suitable IdP.

To configure Login Discovery for My Domain, create a handler in Apex and then reference the handler from the My Domain Setup page. The Apex class implements the `MyDomainLoginDiscoveryHandler` interface. The handler includes logic that defines how to look up a user based on the identifier value entered on the login page. Then it determines which authentication service to invoke.

1. From Setup, enter `My Domain` in the Quick Find box, and then select `My Domain`.
2. Under Authentication Configuration, click `Edit`.
3. For Login Page Type, select `Discovery`.
4. Optionally, for Login Prompt, enter the text or custom label. For example, you can use a custom label to localize the text, for example, `$Login.loginPrompt`.
5. Locate the Login Discovery Handler that you created by implementing the `MyDomainLoginDiscoveryHandler` interface. From Setup, enter `Apex Classes` in the Quick Find box, and then select `Apex Classes`. Select the handler from the list.
6. Optionally, for Execute Login As, choose a Salesforce admin with Manage Users permission. By default, the handler runs in system mode.
7. Click `Save`.

**Troubleshooting tip:** If you’re trying to set up Login Discovery and can’t log in, modify the URL to return to the standard login page, which prompts for a username and password. You can add `login` as a URL query string parameter, for example, `https://northerntrailoutfitters-dev-ed.my.salesforce.com/?login`. Or you can add `login=true` to the URL, for example, `https://northerntrailoutfitters-dev-ed.my.salesforce.com/?login=true`.

---

**Best Practices for Implementing My Domain**

<table>
<thead>
<tr>
<th>If You Have the Following</th>
<th>Do the Following</th>
</tr>
</thead>
<tbody>
<tr>
<td>API integrations into your org</td>
<td>Check whether the API client references the server endpoint. For the API client, use the <code>LoginResult.metadataServerUrl</code> value returned by the login request. Don’t use a hard-coded server URL. After you deploy your subdomain, Salesforce returns the server URL containing your subdomain name. Redirect policy settings have no effect on API calls, so old calls to instance URLs continue to work. However, best practice is to use the value returned by Salesforce.</td>
</tr>
<tr>
<td>Email templates</td>
<td>Replace references to the org’s instance URL with your subdomain.</td>
</tr>
</tbody>
</table>

**Available in:** both Salesforce Classic and Lightning Experience

**Available in:** Essentials, Performance, Unlimited, Enterprise, Developer, Professional, and Group Editions
If You Have the Following
Custom Visualforce pages or custom apps
Chatter
Zones for Communities (Ideas/Answers/Chatter Answers)

Do the Following
Replace references to the org’s instance URL with your subdomain. For details, search for “hard-coded references” in Salesforce Help.
Tell your users to update all bookmarks listed on their Chatter groups.
Update the email notification URL.

Get System Performance and Maintenance Information with My Domain

You can get information about system performance and availability from trust.salesforce.com. Trust reports status information based on your org instance. If you’re using My Domain and don’t know your org instance, you can look it up.

Here’s how to get status information using your domain name.

2. Under System Status, click Learn More.
   The Status & Maintenance page shows the status for each org instance.
4. At the top right of the page, click My Domain.
5. Enter your domain name in the search bar to get your org instance. Don’t enter the complete URL. For example, use yourDomain, not https://yourDomain.my.salesforce.com/.
6. Under Status & Maintenance, select All, and look for your instance.
CHAPTER 4 Configure and Use the App Launcher

In this chapter ...

• Set the Default Sort Order for Apps
• Make the App Launcher the Default Landing Page
• Enable the App Launcher with a Profile in Salesforce Classic
• Enable the App Launcher with a Permission Set in Salesforce Classic

The App Launcher is how users switch between apps. It displays tiles that link to a user’s available Salesforce, connected (third-party), and on-premises apps. You can determine which apps are available to which users and the order in which the apps appear. You can also make the App Launcher the default landing page when users first open Salesforce.

The App Launcher is available to all Lightning Experience and Salesforce Classic users.

The App Launcher is useful for managing access to connected apps. And you can use the AppMenuItem API to control the apps in the App Launcher programmatically.

App Launcher in Salesforce Classic

The App Launcher is an integral part of Lightning Experience and all users can easily access it. However, a few steps are required to set up App Launcher in Salesforce Classic.

To learn more about using the App Launcher in Salesforce Classic, watch Setting up 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 that they are authorized to see according to their profile or permission sets. For profiles, see Enable the App Launcher with a Profile in Salesforce Classic. For permission sets, see Enable the App Launcher with a Permission Set in Salesforce Classic.

Note: In Salesforce Classic, Salesforce admins using the System Administrator profile have access to the App Launcher. Admins using profiles cloned from the System Administrator profile don’t.
Set the Default Sort Order for Apps

As a Salesforce admin, you control the initial sort order of the Salesforce standard, custom, and connected apps that your users see in your org. You can also hide apps so that they don’t show in the App Launcher.

Users can rearrange the apps in their App Launcher to their liking. Their sort order overrides yours. As a Salesforce admin, you can change the order in which apps appear in the Lightning Experience App Launcher. Users can then reorder their personal view of the App Launcher to their liking.

Apps in the App Launcher appear as large tiles and link to Salesforce standard apps, custom apps, and connected apps. Connected apps are third-party apps, such as Google’s G Suite, that you install for your users’ convenience. By installing connected apps, your users can access them from one place and without having to log in again.

To make connected apps and service providers appear in the App Launcher, specify their start URL in the App Manager. The start URL takes users to a specific location after authenticating.

IN THIS SECTION:

Reorder App Launcher Apps in Lightning Experience
As a Salesforce admin, you can change the order in which apps appear in the Lightning Experience App Launcher. Users can then reorder their personal view of the App Launcher to their liking.

Reorder the App Menu and App Launcher in Salesforce Classic
You can change the order in which apps appear in the app menu and App Launcher. The app menu is a dropdown in the upper-right corner of every page in Salesforce Classic. If enabled, the App Launcher is listed in the dropdown menu.

Reorder App Launcher Apps in Lightning Experience

As a Salesforce admin, you can change the order in which apps appear in the Lightning Experience App Launcher. Users can then reorder their personal view of the App Launcher to their liking.

1. From Setup, enter App Menu in the Quick Find box, then select App Menu.
2. From the list of app menu items, drag the apps to change their order. Changes take effect immediately.
3. Optionally, click Visible in App Launcher or Hidden in App Launcher to show or hide individual apps from the App Launcher for all users in the org.

Note: By default, all standard and custom apps are visible in the App Launcher. If you want to change the default behavior to hide all standard and custom apps, contact Salesforce Customer Support.

All apps installed in the org appear on the app menu items list. However, the apps that users see in their app menu and App Launcher vary depending on each app’s visibility settings and the user’s permissions. Users see only the apps that they are authorized to see according to their profile or permission sets.

Your users can reorder apps in their App Launcher, and their sort order overrides the order that you set here.

To view apps:
- View Setup and Configuration

To manage apps:
- Customize Application

User Permissions

To view apps:
- View Setup and Configuration

To manage apps:
- Customize Application

Editions
Available in: both Lightning Experience and Salesforce Classic

Available in: Contact Manager, Group, Professional, Enterprise, Performance, Unlimited, and Developer Editions
Reorder the App Menu and App Launcher in Salesforce Classic

You can change the order in which apps appear in the app menu and App Launcher. The app menu is a dropdown in the upper-right corner of every page in Salesforce Classic. If enabled, the App Launcher is listed in the dropdown menu.

Apps in the App Launcher appear as large tiles and link to Salesforce standard apps, custom apps, and connected apps. The App Launcher displays a user’s available Salesforce apps and the connected apps that a Salesforce admin installs for the org.

1. From Setup, enter **App Menu** in the Quick Find box, then select **App Menu**.
2. From the list of app menu items, drag the apps to change their order. Changes take effect immediately.
3. Optionally, click **Visible in App Launcher** or **Hidden in App Launcher** to show or hide individual apps from the App Launcher for all users in the org.

The app menu lists all apps installed in the org. However, the apps that users see in their App Launcher vary. You control each app’s visibility settings and users’ permissions.

Follow these steps to set the initial ordering of apps on the app menu. If your users reorder apps in their App Launcher, their sort order overrides yours. Also, after a user reorders the apps, the Salesforce Classic app menu displays the apps in the user’s preferred order.

Make the App Launcher the Default Landing Page

Make it easy for your Salesforce Identity users to access what they need by presenting the redesigned App Launcher as the default landing page when they log in to Salesforce.

**Note:** These steps work in Lightning Experience. If you see the App Launcher icon () on the left side of the navigation bar at the top of your screen, you’re in Lightning Experience. If not, you’re in Salesforce Classic.

1. From Setup, enter **App Manager** in the Quick Find box, then select **App Manager**.
2. Click **New Lightning App** and walk through the New Lightning App wizard. Add only the App Launcher tab to Selected Items.
3. Make the App Launcher the default when users log in for the first time.
   a. From Setup, enter **Profiles** in the Quick Find box, then select **Profiles**.
   b. Select a profile and scroll to the Custom App Settings section.
   c. Select **Default** next to the Lightning app.
4. Log out and log in again.
   The new Lightning app appears in the navigation bar and App Launcher.
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.

Note: These steps work in Salesforce Classic. If you see the App Launcher icon (ображення) on the left side of the navigation bar at the top of your screen, you’re in Lightning Experience. If not, you’re in Salesforce Classic.

In Salesforce Classic, Salesforce admins using the System Administrator profile have access to the App Launcher. Admins using profiles cloned from the System Administrator profile don’t.

1. From Setup, enter Profiles in the Quick Find box, then select Profiles.
2. Click New Profile.
3. Select an Existing Profile as a basis for the new profile.
   For example, select Standard User.
4. Enter the name of the new profile.
   For example, Standard User Identity.
5. Click Save.
6. In the detail page for the new profile, click Edit.
7. In Custom App Settings, set the App Launcher to Visible, if it isn’t already.
   Under Tab Settings, verify that the App Launcher tab is set to Default On.
8. Under Administrative Permissions, select Use Identity Features.
9. Click Save.
10. From Setup, enter Users in the Quick Find box, then select Users.
11. Click Edit next to each user you want to access the App Launcher.
12. In the user’s Profile field, select the new profile that has “Use Identity Features” enabled.
   For example, you might use the Standard User Identity profile.
13. Click Save.
   When you log in as the selected user, the App Launcher appears in the drop-down app menu.
Enable the App Launcher with a Permission Set in Salesforce Classic

Create a permission set and assign it to users so that they can access the App Launcher.

Note: These steps work in Salesforce Classic. If you see the App Launcher icon (определен) on the left side of the navigation bar at the top of your screen, you’re in Lightning Experience. If not, you’re in Salesforce Classic.

1. From Setup, enter Permission Sets in the Quick Find box, then select Permission Sets.
2. Click New.
3. Enter a label for the new permission set.
   For example, Identity Features.
4. Optionally, restrict the use of the permission set to a specific user license.
5. Click Save.
6. Click System Permissions.
7. Click Edit, and select Use Identity Features.
8. Click Save.
9. From Setup, enter Users in the Quick Find box, then select Users.
10. Click the name of the user to whom you want to give access to the App Launcher.
11. In the Permission Set Assignments related list, click Edit Assignments.
12. Add the permission set that you created to Enabled Permission Sets.
13. Click Save.

When you log in as the selected user, the App Launcher appears in the dropdown menu.

Note: Still not seeing the App Launcher? In the profile associated with the user, select Visible for the App Launcher setting.
You can set up single sign-on (SSO) so that users can access Salesforce without logging in again. This mechanism is called inbound SSO. Likewise, you can set up outbound SSO so that users who are logged in to Salesforce can access third-party apps and other services without logging in again.

Salesforce supports SSO from third-party identity providers. For SSO to work, you need an identity provider and a service provider to coordinate authentication and authorization information using SAML assertions.

For more information about SSO, refer to these resources:

- For an overview about how to set up and troubleshoot SSO, watch this video: Setting Up Single Sign-On (23:31 minutes).
- For a tutorial about setting up SSO for your org, go to Trailhead: Set Up Single Sign-On for Your Internal Users.
- For in-depth information, check out the SSO Implementation Guide, Salesforce Single Sign-On Implementation Guide.
CHAPTER 6 Two-Factor Authentication

Two-factor authentication is the most effective way to protect your org’s user accounts. As a Salesforce admin, amplify 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.

Two-factor authentication is an essential user authentication method—so essential that Salesforce provides two types of two-factor authentication.

- **Service-based**—Also known as device activation, service-based two-factor authentication is automatically enabled for all orgs.
- **Policy-based**—Admins enable policy-based two-factor authentication. It is an admin’s best tool to protect org user accounts.

For help with configuring two-factor authentication, see the Admin Guide to Two-Factor Authentication and the Trailhead Module Secure Your Users’ Identity.

### Org Policies That Require Two-Factor Authentication

Set policies that require a second level of authentication for every login, for logins through the API (for developers and client applications), or for access to specific features. Users provide the second factor by downloading and installing a mobile authenticator app, such as the Salesforce Authenticator app or the Google Authenticator app, on their mobile device. They can also use a U2F security key as the second factor. After users connect an authenticator app or register a security key with their Salesforce account, they can use these authentication methods whenever your org’s policies require two-factor authentication.

The Salesforce Authenticator mobile app (version 2 and later) sends a push notification to the user’s mobile device when the Salesforce account requires identity verification. The user responds on the mobile device to verify or block the activity. The user can enable location services for the app and automate verifications from trusted locations, such as a home or office. Salesforce Authenticator also generates verification codes, sometimes called “time-based one-time passwords” (TOTPs). Users can choose to enter a password plus the code instead of responding to a push notification from the app for two-factor verification. Or they can get a verification code from another authenticator app.

If users lose or forget the device they usually use for two-factor authentication, you can generate a temporary verification code for them. You set when the code expires, from 1 to 24 hours after you generate it. Your user can use the code multiple times until it expires. A user can have only one temporary
Two-Factor Authentication

code at a time. If a user needs a new code while the old code is still valid, you can expire the old code, then generate a new one. Users can expire their own valid codes in their personal settings.

SEE ALSO:

Salesforce Help: Personalize Your Salesforce Experience
Set Up Two-Factor Authentication
In this chapter ...

• Identity Connect
• Install Identity Connect

Use Identity Connect to upload and synchronize user data from Active Directory to Salesforce. Identity Connect includes an administration console for managing and synchronizing users. You can set up single sign-on using Identity Connect so that users who sign into their desktop environment can use Salesforce without logging in separately.

For details on Identity Connect, see the Salesforce Identity Connect Release Notes and User Guide.

To test Identity Connect, sign up for a Salesforce trial.

To learn how to download and install Identity Connect to synchronize your Active Directory users with your Salesforce users, watch Integrating Active Directory with Salesforce using Identity Connect.

For more in-depth learning, see the Trailhead module, Identity Connect Basics.
Identity Connect

Identity Connect integrates Microsoft Active Directory (AD) with Salesforce. User information entered in AD is shared with Salesforce seamlessly and instantaneously. Companies that use AD for user management can use Identity Connect to manage Salesforce accounts.

Changes in AD are reflected in Salesforce in near real time. For example, when a user is created in AD, the Salesforce user account is created as part of the provisioning process. When deprovisioned, the user’s Salesforce session is revoked immediately.

You can also use Identity Connect for single sign-on to Salesforce.

Identity Connect runs as a service on either Windows or Linux platforms.

Install Identity Connect

Your org must have at least one Identity Connect license. To obtain Identity Connect, contact Salesforce.

Identity Connect is typically installed on a server by your IT department. Each user doesn’t 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 org.

2. Click the download link that corresponds to your operating system.

While Salesforce Identity maintains the identity of your internal users (employees), Salesforce External Identity provides similar services to external users, such as customers, purchasers, patients, partners, and dealers. This product, also called Salesforce Identity for Customers and Partners, improves your engagement with your external users. With little effort on your part, you can provide your external users a login page that reflects your brand. You can further customize the login process with the provided tools.

External Identity License Details

The Salesforce External Identity User license lets you deliver identity services, including single sign-on (SSO), to your customers and partners. It is a standalone license that you can buy for blocks of users who are consumers of your business, such as customers, purchasers, patients, partners, and dealers.

With the External Identity license, you can store and manage customers and partners. You can authenticate external users through a username and password or SSO. You can also authenticate users with a passwordless login, such as with a verification code sent in an email or text message, a social identity provider, Salesforce Authenticator, or a physical device, like a Yubikey. You can also use these identity verification methods as a second factor (2FA). External Identity supports self-registration to provision new users easily.

You can upgrade the External Identity User license to a Customer Community or Partner Community license to benefit from Community features.

The External Identity User profile defines a set of object permissions that you can assign to an external identity user. To modify the External Identity User profile, clone the default External Identity User profile, and edit the profile as needed.

Note: To prevent unintended data leaks, the default External Identity User profile contains a more limited set of object permissions than what is available with the license. For example, users can read accounts but not update them. Users can read and update contacts and individuals but not create them. You can increase object access by cloning the default profile and changing object permissions as needed. This stricter default profile impacts external identity users as of Spring ’19 and applies only to new orgs. External identity users provisioned before Spring ’19 aren’t affected.

This table lists the object permissions that you can assign to External Identity users.

<table>
<thead>
<tr>
<th>Accounts</th>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
<th>Default Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>Read</td>
</tr>
<tr>
<td>Assets</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cases</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chatter</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contacts</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>Read, Update</td>
</tr>
<tr>
<td>Documents</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Files</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Household</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>Not Available</td>
</tr>
<tr>
<td>Ideas</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Individuals</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>Read, Update</td>
</tr>
<tr>
<td>Knowledge</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Party-Related Party</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>Not Available</td>
</tr>
<tr>
<td>Party Relationship</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>Not Available</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td>Read</td>
<td>Update</td>
<td>Delete</td>
<td>Default Profile</td>
</tr>
<tr>
<td>------------------</td>
<td>--------</td>
<td>------</td>
<td>--------</td>
<td>--------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Plan Benefit</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>Not Available</td>
</tr>
<tr>
<td>Plan Benefit Item</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>Not Available</td>
</tr>
<tr>
<td>Price Books</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Products</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Orders</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Questions and Answers</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>Not Available</td>
</tr>
<tr>
<td>Solutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tasks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work Orders</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Objects</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Ten custom objects per profile, but custom objects in managed packages don't count toward this limit</td>
</tr>
<tr>
<td>Additional Storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>150 MB (25,000 active users)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2 GB (250,000 active users)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10 GB (1,000,000 active users)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>60 GB (5,000,000 active users)</td>
</tr>
</tbody>
</table>

We recommend that the number of External Identity license users in your external identity community not exceed ten million unique users per month. If you require additional user licenses beyond this limit, contact your Salesforce account executive. Exceeding this limit can result in an extra charge and decrease expected functionality.
Monitor connected apps and set up reports to track app usage by user, app, time, or other values.

After you've set up connected apps for your Identity users, you can monitor the usage of connected apps throughout your org. You can find out how often the apps are used, change connected app settings, and block or unblock apps as your security needs change.
Monitor Usage for Connected Apps

Salesforce admins can monitor installed connected apps from the Connected Apps OAuth Usage page in Setup.

To view information about OAuth connected apps, from Setup, enter OAuth in the Quick Find box, then select Connected Apps OAuth Usage. The resulting list of apps can be long because it contains all Salesforce and custom OAuth apps available to your users, not just the ones installed in your org. For example, it lists apps from AppExchange and Salesforce partners.

### Connected Apps OAuth Usage

Manage OAuth connected apps in use in this org. Install apps to manage policies. Block apps to prevent new sessions with the connected app. Existing sessions are unaffected.

<table>
<thead>
<tr>
<th>Connected App</th>
<th>Description</th>
<th>Manage App Policies</th>
<th>User Count</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Manager</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity Editor for Heroku</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analytics for iOS</td>
<td>The &quot;Analytics for iOS&quot; Connected App allows mobile clients to easily connect to your org, and it gives administrators control over who's logging in and how mobile clients can share images and links.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anypoint Data Gateway Designer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anypoint Platform Employee</td>
<td>Manage App Policies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AppExchange</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Tokens</td>
<td>Manage App Policies</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Connected App**

Name of the connected app. The list contains only the apps that users in the org are using. These apps have an active access or refresh token.

**Description**

Description of the connected app.

**Manage App Policies**

Click Manage App Policies to open the detail page for the connected app. From the detail page, you can click Edit Policies to manage the app’s access and security policies.

**User Count**

Number of users who are using the app. Click a User Count number to open the Connected Apps User's Usage page to see information about users, including:

- When they first used the app
- Most recent time they used the app
- Total number of times they used the app
From this page, you can end a user’s access to the current session by clicking Revoke. Or, you can click Revoke All at the top of the page to log out everyone currently using the app.

Actions
You can perform one of the following actions.

- **Install**—Make the OAuth connected app available for access and security policy management. When you click install, the Manage App Policies link appears next to the app. Click the link to open the app’s detail page where you can set policies. Install appears next to apps that were created in another org but you can’t manage their policies in your org.

- **Uninstall**—Remove the local copy of the OAuth connected app. Click uninstall only when the original developer deletes the app in the other Salesforce org. Uninstall doesn’t remove the connected app. It just removes the local copy that you installed to set the app’s OAuth policies in your org. By uninstalling the app, you’re only removing the OAuth policies that you set for the app. You’re actually loosening your security measures because you’re removing the policies for apps that users can still access.

- **Block**—Make the OAuth connected app inaccessible to your org’s users. Blocking an app ends all current user sessions and prevents future sessions until you click Unblock.

- **Unblock**—Give users access to the connected app. By unblocking the app, users can log in and run the app. If Unblock is disabled, the app is blocked org-wide because it’s not whitelisted. To whitelist the app, click Install. Then click Edit Policies, and under the app’s OAuth settings, set Permitted Users to Admin approved users are pre-authorized. You can whitelist apps only if you’ve asked Salesforce to enable the API client whitelisting feature.

---

Salesforce maintains Identity event logs that you can use to create reports and dashboards to provide information about single sign-on and connected app usage.

Follow these steps to set up a report about Identity users. After that, you can create the same steps to set up more than one variation of the same report type, or create a dashboard for the report. For more information, see “Get Started with Dashboards” in Salesforce Help.

**Note:** Single Sign-On and Access Management for Mobile Applications (13:17 minutes)

Learn how to create reports for monitoring mobile Identity users and usage. First, this video covers creating and deploying mobile connected apps. Then, it shows how to set up reporting for connected apps usage.

**Establish a new report type**

1. From Setup, enter Report Types in the Quick Find box, then select Report Types.
2. Click New Custom Report Type.
3. Enter the following values.
   a. Primary Object: Users
   b. Report Type Label: A unique label, such as Identity Users
   c. Report Type Name: This field automatically uses the label; change it if you want a different name.
   d. Description: Give it a useful description.
   e. Store in Category: Pick a category for this report, such as Administrative Reports.
   f. Deployment Status: Keep as In Development until you’re ready to deploy this report for other users to see.
4. Click Next.
5. Select Click to relate to another object.
6. Select **Identity Event Logs (Users)**.

7. Click **Save**.

   a. From App Launcher, search for Reports.
   b. Click **New Report**.
   c. For Report Types, select **Identity Users**.
   
   ![Diagram of Identity Event Logs (Users) report]

   **Note:** A new report opens for editing. If you don’t get any results, click **All Time**.

d. Under Columns, select fields to get Identity information, such as Username, User ID, Identity Used, App: Connected App Name, Timestamp, and User Type.

e. Click **Save** and name the report.
   f. Click **Save**, or click **Save and Run Report** to see the results immediately.

9. Create a dashboard based on your report.

   **Example:** Here’s a dashboard based on a few identity-related reports.
Here are more sources of information about Salesforce Identity.
Salesforce Identity also supports external identities for partners and customers.

Use the following links for other useful resources.

- Salesforce Identity product page
- Trailhead: Identity Basics
- Trailhead: User Authentication
- Salesforce Identity "How To" videos
- Security Single Sign-On Implementation Guide
- Understanding Authentication in the REST API Developer Guide
- Salesforce Identity Connect Release Notes and User Guide
INDEX

A
Active Directory 21–22
App Launcher
  configure 13

E
External Identity license 24
external identity provider 18, 23

I
Identity
  links to more information 31
  monitor 27
  overview 1
  reports 26, 28
  scenario 3
Identity Connect 21

L
license 24

P
Password
  change user 19
  identity verification 19
  login verification 19
  two-factor authentication 19
permission set licenses 22
Permission set licenses 22
product overview 1

T
Two-factor authentication 19

U
User setup
  change password 19