**What Does Salesforce Identity Do?**

Salesforce Identity lets you give the right people the right access to the right resources at the right time. You control who can access your orgs and who can use apps running on the Salesforce Platform, on-premises, in other clouds, and on mobile devices.

When users can sign in once to access all the apps that they need, everyone benefits.

* Users don’t have to remember lots of usernames and passwords.
* Admins spend less time dealing with user login woes.
* Developers build web and mobile applications that work seamlessly with existing business processes.
* CIOs strengthen security and trust while harnessing their authentication investment.
* Customers collaborate and get their questions answered without hassle.
* Partners integrate their solutions with your Salesforce org, making it a big win for everyone.

## What Does “Identity” Mean Anyway?

In the tech industry, identity is a loaded term and has different meanings depending on the context. But generally, identity has come to mean that identity providers ensure that people are who they say they are.

At Salesforce, we’re talking about digital information about users, like who the user is and what the user can do in a particular context. It can also include attributes about the user, such as first and last names, contact information, maybe even a job title.

## What Features Does Salesforce Identity Provide?

## Single Sign-On

Single sign-on (SSO) lets users access all authorized resources without logging in separately to each one—and without having to create (and remember) different user credentials for each app.

You can connect your users to several accounts and applications running in other Salesforce orgs and even in other clouds. For example, a call center rep with Salesforce Identity can click a link and be logged in immediately to other apps, like Google Apps, Microsoft Office 365, or Box.

## Connected Apps

And what are those “authorized resources” that your signed-on users have access to? You got it: They’re connected apps. Connected apps bring Salesforce orgs, third-party apps, and services together. If a connected app is created without implementing SSO, it acts like a bookmark. Users can get to the app from the App Launcher or dropdown app menu, but they sometimes have to sign in again to use it.

So to get the most out of connected apps, configure them for SSO. With SSO, admins can set security policies and have explicit control over who uses which apps. You can also use connected apps to manage authentication and policies for mobile applications.

## Social Sign-On

Social sign-on sounds a lot like single sign-on, doesn’t it? It’s easy to confuse the two, not only because the terms are similar, but also because both features make users’ lives easier.

With social sign-on, users log in to a Salesforce org with their username and password from an external authentication provider, like Facebook, Twitter, LinkedIn, or Google. You can set up any of these providers with a few clicks. With a little bit of work, you can set up other providers, like PayPal and Amazon.

Social sign-on is especially useful when you want customers to be able to log in to a community without having to create (and remember) a new username and password. Customers can log in to a Salesforce community using their Facebook or LinkedIn account.

## Multi-Factor Authentication

Until now, we’ve been talking about features that make it easier for your users to access the orgs and apps they need to do their jobs. Initially, multi-factor authentication makes access a little more difficult, but this simple yet powerful tool strengthens user account security.

When you enable multi-factor authentication, users have to provide two or more pieces of evidence—or factors—when they log in. One factor is the user’s username and password combination. The requirement for additional factors is satisfied through the use of a verification method that the user has in their possession, such as an authenticator app or a Universal Second Factor (U2F) security key.

With the newest version of the Salesforce Authenticator app, the second factor can be a response to a push notification on the user’s mobile device.

Multi-factor authentication helps ensure that even if an attacker acquires a user’s password, the attacker can’t log in and do harm. So while you’re expanding your authentication options with other Salesforce Identity features, be sure to secure individual access to your org with multi-factor authentication.

## My Domain

Would you like the URL to your Salesforce org to be something that makes sense to your users? Well, you can make that happen. With the My Domain Identity feature, you can customize your Salesforce URL to include your company or brand name. For example, if you work for Jedeye Technologies, you can include the name in your Salesforce login URL: https://jedeye-tech.my.salesforce.com.

Notice that the URL ends in salesforce.com. With My Domain, you’re actually creating a subdomain within the Salesforce domain, salesforce.com.

Having a My Domain isn’t just about convenience and branding your org’s login experience. It's about having more control over your login process and simplifying authentication. In fact, Salesforce requires you to have a My Domain in place to:

* Work in multiple Salesforce orgs in the same browser
* Set up single sign-on (SSO) with external identity vendors
* Set up authentication providers, such as Google and Facebook, so that your users can log in to your Salesforce org with their social account credentials
* Use Lightning components in Lightning component tabs, Lightning page, the Lightning App Builder, or standalone apps

Because having a My Domain is so important, all production and Developer Edition orgs created in Winter ’21 and later get one by default. If you don’t like your org’s My Domain name, you can change it.

## Centralized User Account Management

Centralized user account management means that admins can manage all their user account tasks in one place. Administrators can easily grant users access to other apps and revoke or freeze access when they have to.

Admins can apply login policy and explicit security controls. For example, they can set a policy that prevents login attempts by anyone who doesn’t know your domain name.

Centralized user account management is good for users, too. They don’t have to remember so many usernames and passwords. No more sticky notes dangling from monitors. In short, centralized management provides greater control over security, helps reduce access-related risk, and makes life easier for end users.

## User Provisioning for Connected Apps

Want to create, manage, and secure user accounts across all your orgs and connected apps? That’s what Salesforce Identity user provisioning does for you. You can manage user information quickly, cheaply, reliably, and securely across multiple systems and connected applications.

Many people with Salesforce accounts also have accounts in other clouds, such as Google Apps, Office365, Concur, or Box. Salesforce user provisioning provides a single location where admins can create, update, delete, and manage those user accounts.

## Identity Connect

Salesforce Identity Connect synchronizes users and their attributes from Active Directory (AD) to Salesforce. When a user is created in AD, that same user account can also be created automatically in Salesforce. When a user is deleted from AD, the user account in Salesforce is deactivated at the same time.

With Identity Connect, you can let users sign in to Salesforce using their AD username and password. In some circumstances, you can configure Identity Connect to automatically sign users in to Salesforce. Yup—users can click a bookmark or link to Salesforce and they’re authenticated and taken to Salesforce without even seeing a login page. Users love this!

A future module helps you decide whether Identity Connect is right for you.

## App Launcher

The App Launcher is part of Salesforce Identity and it plays a prominent role in Lightning Experience. The App Launcher presents tiles for all the standard apps, custom apps, and connected apps in your Salesforce org. Your users can go to one location in Salesforce to access all apps—without having to log in again. You choose which third-party and other connected apps to add the App Launcher. And you control which apps are available to which users.