**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.

As a Salesforce admin, you get it. You understand that for your coworkers to be as productive as possible, they need a simple, secure way to access your Salesforce org and other apps and services.

That simple, secure way is Salesforce Identity. With Salesforce Identity, you can remove barriers that slow employees down while maintaining robust security controls. Here are some key benefits for employees, for you, and for your company.

**Convenience**

Employees can log in to a workstation and connect to a Salesforce org without logging in again. In fact, they can have a single login that works for all their web and mobile apps. You can give them one-click access to third-party productivity tools and services, like Gmail or Microsoft Office 365.

Yes, you heard that right: one click. No additional login required. And as your company implements new services, you can give employees easy access to those as well. Just add everything to the Salesforce App Launcher. The App Launcher gathers all the apps an employee needs in one place—each app is just a click away.

**Control**

Managers and supervisors can have more control over their employees. If you want fine-grained control over who uses what, you can require that a manager or supervisor approve employee requests to access an app or service. And when you need to revoke access to an app, you can do that, too.

**Security**

The magic of Salesforce Identity is that more convenience plus greater control adds up to enhanced security. One identity source for user credentials across corporate networks and the web makes it easy for you and other Salesforce admins to monitor and manage usage. Reduce redundant accounts, and you reduce your vulnerability to malicious activity.

And with multi-factor authentication, you can be twice as confident that your users are who they claim to be.

Here are some key benefits of Salesforce Identity for customers and partners and for your company.

**User Registration**

When you want customers and partners to register to use your org or community, you can customize the registration process. During registration, you can collect vital pieces of information to personalize the user experience, such as a location, contact preferences, or profile photo. Users can easily edit that information later to keep it up to date. Because Salesforce Identity is part of the Salesforce Platform, you can launch workflows and other business processes right from user registration.

**Brand Control**

Your company needs to control its brand during every stage of a user journey, from registration to login and beyond. You want customers and partners to encounter *your* corporate brand, not ours. You can configure Salesforce Identity so that your customers and partners never guess that Salesforce is behind the experience. Salesforce Identity helps you create a user journey within your own brand.

**Social Sign-On**

Some customers don’t want to scribble yet another username and password on the sticky note dangling from their monitor. Instead, they’d rather sign in to your site using their credentials from Facebook, LinkedIn, Twitter, or another social provider. Salesforce Identity offers out-of-the-box social sign-on capabilities for popular social networks.

It also supports OpenID Connect–based providers.

And if you’re up for a bit of coding, you can create a custom authentication provider plug-in to authenticate users with any provider that uses OAuth. As icing on the cake, Salesforce can use the social sign-on process to register new user accounts automatically, without requiring the customer to fill in a form.

**Seamless Web Experience**

Your company’s online customer experience likely includes a mix of Salesforce and non-Salesforce web content, services, and apps. Because Salesforce Identity provides SSO for customers and partners, they can move seamlessly between your company’s sites and a third-party website without encountering disruptive login screens.

**One Comprehensive Picture of the User**

Salesforce Identity is part of the Salesforce Platform. It harnesses the power of the platform to give a complete and consistent picture of each customer to multiple divisions of your business. For example, you can configure social sign-on to create both a new user and an associated contact record. Then you can kick off an email communication campaign to drive engagement. Or you can open a task to remind an account executive to give the new user a welcome call.

## Identity Standards and Protocols

Here are the three protocols that Salesforce and other identity vendors follow to implement identity solutions.

* SAML
* OAuth 2.0
* OpenID Connect

**SAML Protocol**

When you want users to move seamlessly between Salesforce orgs and applications without logging in repeatedly, you set up single sign-on (SSO). Security Assertion Markup Language (SAML) is the protocol that makes it happen.

Here are a couple of examples of SAML in action.

* When you’re logged in to Salesforce and then click the App Launcher to get directly to your Gmail inbox, that’s SAML in action.
* When users who are already logged in to another app can access their Salesforce org without logging in again, that’s also SAML in action.

## SAML Assertion

This is how SAML works. A user tries to access a service. The service provider sends out a request to the identity provider basically asking, “Hey, is it okay if this user accesses my service?” The identity provider makes sure that users are who they say they are by checking its database and then returning a response—an assertion—saying, “Yes, this user is authorized, and here’s some information about the user.”

Wait a minute. What’s the difference between an identity provider and a service provider? Basically, the identity provider is the one authenticating the user. The service provider is asking for the authenticated identity.

The assertion is the information being sent. An assertion can carry detailed information about a user. It can also contain attributes about the user, like first and last names, contact information, maybe even the job title.

SAML happens in the background. Your users don’t see any of it. They just click an icon or link and open another app without having to provide additional information or log in again. Sometimes their destination already knows something about them (those user attributes) when they get there.

## SAML and XML

SAML is an XML-based protocol, which means that the packages of information being exchanged are written in XML. XML is supposed to be (almost) human-readable so that you can get some idea of what’s going on. That’s good news when you’re trying to figure out if things are working correctly.

## OAuth 2.0 Protocol

OAuth 2.0 is an open protocol used to allow secure data sharing between applications. The user works in one app but sees the data from another. For example, you’re logged in to your Salesforce mobile app and see your data from your Salesforce org.

Behind the scenes, the apps perform a kind of handshake and then ask the user to authorize this data sharing. When developers want to integrate their app with Salesforce, they use OAuth APIs.

## OpenID Connect Protocol

The OpenID Connect protocol adds an authentication layer on top of OAuth 2.0 to enable secure exchange of user information. Like SAML, OpenID Connect sends identity information from one service to another. Unlike SAML, OpenID Connect is built for today’s world of social networks. Have you ever installed a new app and come across a prompt like "Log in with your Google account"? That app is using the OpenID Connect protocol. When you sign in with Google, you’re not creating an account and another password. Only Google holds that information.

For instance, when Google verifies a user’s identity on behalf of another service, it’s authenticating the user. In this way, Google is an identity provider.

The advantage of the OpenID Connect protocol for users is that they can reduce the number of separate accounts, usernames, and passwords. On the flip side, developers can authenticate their users across websites and apps without having to own and manage password files. This process makes it that much harder for hackers to compromise user accounts.

## SAML Flow for SSO

The SSO process all happens with lightning speed, but a few steps are involved.

1. The user tries to access Salesforce.
2. Salesforce recognizes the SSO request and generates a SAML request.
3. Salesforce redirects the SAML request back to the browser.
4. The browser redirects the SAML request to the external identity provider.
5. The identity provider verifies the user’s identity and packages the SAML assertion containing the user authentication.
6. The identity provider sends the SAML assertion to the browser.
7. The browser redirects the assertion to Salesforce.
8. Salesforce verifies the assertion.
9. The user is now signed in and can access Salesforce.

## Identity Terminology Cheat Sheet

How’s that for a crash course on the topic of identity protocols? When words sound similar and differences are nuanced, it can be hard to keep them straight. So here’s a cheat sheet. Hope it helps!

| **One Term** | **That’s Easily Confused with This Term** |
| --- | --- |
| **Authentication** means who a person is. These days, authentication is often used as shorthand for authorization and authentication. | **Authorization** means what a person can do. |
| **Protocol** specifies the set of rules that enable systems to exchange information. Generally, the term protocol and standard are used interchangeably. | **Standard** is a specification, a set of industry practices that vendors agree to support. Often, a standard contains a protocol to specify how the companies implement the standard. |
| **Username and password** are what the user supplies to log in to a system. | **Credentials** are basically the same thing. |
| **Single sign-on (SSO)** enables a person to log in once and access other apps and services without logging in again. | **Social sign-on** enables a person to log in to an app using the credentials established with a social account like Google. That app accepts the Google credentials, and the user doesn’t have to create another account and password. |
| **Identity provider** is a trusted service that enables users to access other websites and services without logging in again. | **Service provider** is a website or service that hosts apps and accepts identity from an identity provider. |