okta

Three Ways to Integrate Active Directory with Your SaaS Applications

Okta Inc.
301 Brannan Street
San Francisco, CA 94107

info@okta.com
1-888-722-7871

Contents

1 User Management Challenges of Software as a Service
1 The Importance of Active Directory Integration
2 Option 1: Independent Integrations with AD
2 Option 2: Leverage Microsoft's AD FS
3 Option 3: Use a Third-Party Vendor Solution
4 Okta: AD Integration for All Your SaaS Applications
5 Getting Started with Your Free Trial
5 About Okta

Challenges of Software as a Service

The adoption rate of Software as a Service (SaaS) has been dramatic in recent years. Trials of applications like Salesforce.com, WebEx, or NetSuite have transitioned to enterprise-wide deployments, and many organizations have adopted "SaaS first" policies. In fact, Goldman Sachs research 1 indicates that 58% of the small and midsize business (SMB) segment always consider a SaaS option, and 39% prefer it if available.

However SaaS adoption is not without its challenges. The tendency of SaaS applications to be siloed has made managing user access and authorization an increasing challenge. The task of onboarding users is a time-intensive, manual process that involves administrators across multiple departments, which can introduce risk. For example, because there is frequently no central user directory a fired employee's access is often not revoked right away. And while "anytime and anywhere" access can be a boon to productivity, it also poses adoption and security challenges. IT departments must find a way to harness the benefits of SaaS, while minimizing business risk.

The Importance of Active Directory Integration

In most enterprises, Microsoft Active Directory (AD) is the authoritative user directory that governs access to basic IT services such as email and file sharing. Often, AD is also used to control access to a broader set of business applications and IT systems.

SaaS applications are each developed with their own native user directories that control direct access to their individual services. And, because they run outside of the firewall, SaaS applications have traditionally been beyond the reach of Active Directory.

As SaaS application usage grows, this user directory duplication causes complication and hassle—for both IT departments and users. Users have to remember user IDs and passwords not only for their Windows network, but for each SaaS application as well. IT has to create and manage user accounts in both Active Directory and numerous SaaS applications, and must manually map AD users to corresponding accounts in SaaS applications.

Managing multiple separate user directories that are not integrated with Active Directory can easily lead to a set of untenable security and access management challenges. Seamless integration with AD is a must for any solution used to manage access and authorization to SaaS applications.

True integration with Active Directory must address all of these challenges and provide:

- Two-way user and group synchronization: As users and groups are added to and removed from AD, these changes should be reflected in the SaaS applications. In specific cases, SaaS applications should be able to push user profiles and groups to AD.
- Access provisioning and deprovisioning: When a user is added to AD, the relevant SaaS applications should be automatically provisioned and, conversely, when a user is removed from AD, SaaS access should be automatically revoked.
- Single sign-on (SSO): Users should be able to sign on to the Windows network once, and then easily gain access to their SaaS applications without having to enter an additional set of credentials.

There are three different options for integrating Active Directory with SaaS applications that meet the requirements above with varying degrees of success.

Option 1: Independent Integrations with AD

Some of the largest and most established SaaS applications offer their own AD integration tool, or they expose an API that allows you to develop a custom integration with Active Directory yourself. Google Apps, Microsoft Online Services, and Salesforce.com are all prominent examples of this approach, and all have notable issues.

Google Apps Directory Sync provides one-way pushing of users from Active Directory into a Google Apps account. It presents a flexible way to define which users (and user attributes) are imported. However, the setup and administration is completely separate from the Google Apps administration console, which forces admins to manage this from a locally installed utility instead. There is no concept of ongoing synchronization (synchronization must be implemented manually), and more important, this tool does not support single sign-on. To provide SSO, organizations must use yet another third-party solution, which results in two separate administration models and user stores for SSO and user management.

Microsoft Office 365 Directory Synchronization also provides one-way pushing of users from Active Directory into Office 365. Administrators can use this tool to both provision and de-provision users in Office 365 when they are added or removed from Active Directory. Similar to the Google Apps tool, it is decoupled from the primary administration experience and managed via the on-premises utility. It also does not provide SSO, again resulting in two separate administration models and user stores.

Salesforce.com has published APIs that allow you to build proprietary solutions that both push users from AD, and enable users to authenticate against AD when accessing Salesforce.com. However, there is no readily available tool to accomplish either of these tasks, and to meet the integration requirements organizations must make a significant investment in both development and maintenance.

The downsides of integrating AD with these vendor-specific options are clear. At a minimum, organizations must install and maintain tools from each vendor. However if those tools are not available, organizations must develop their own vendor-specific solution. Even after you've developed and installed these solutions you're left with a portfolio of technologies that must be maintained across all of your SaaS applications, which increases IT costs.

Option 2: Leverage Microsoft AD FS

With the launch of Windows Server 2008 R2, Microsoft released Active Directory Federation Services (AD FS) 2.0, which provides an extensible platform for handling single sign-on with applications outside of the firewall. This means organizations can leverage AD FS to address the SSO requirement of an AD integration, but it does not address user synchronization, nor does it address user provisioning or de-provisioning.

When considering AD FS to address SSO needs, it's imperative to consider the platform. As a feature of Windows Server, AD FS was developed to be a platform—not an end-to-end solution for single sign-on needs. Platforms are powerful and flexible, but they require a significant amount of additional work to develop a complete solution.

But AD FS is a free solution, so why wouldn't organizations use it? AD FS–based solutions require hardware and software (there are three server roles that make up AD FS itself: the Federation Service, the Federation Service Proxy, and the web server agent). AD FS also requires custom development and maintenance, and administrative time to understand, configure, and maintain the SSO connections with the target SaaS applications. When you factor in all these requirements, it's clear that a solution based on AD FS is not free.

To configure AD FS you must obtain a valid SSL certificate (self-signed is sufficient for testing, but third-party signed is necessary for production). Setup involves importing the SSL certificate, exporting certificates, and creating shared certificates to establish trust between your AD FS server and the target federation service. When trust is established, you must then generate the claims rules appropriate for authenticating with the target SaaS application.

Claims rules can vary greatly based on the SaaS application the system is integrating with. Administrators must know the Uniform Resource Identifier (URI) of the SaaS application, which claims the application requires, the URL the application should expose to the user, and finally, whether the token should be encrypted. AD FS provides a flexible rule engine that can handle most situations, but you must not only define those rules for every integration, but you must also continuously maintain them as the target SaaS application changes.

Searching blog posts, websites, and technical documentation to discover the appropriate claims rules for each SaaS application is time-consuming and unreliable. The rules for each application may also change over time, invalidating your SSO integration, so tracking those changes is necessary.

Once you establish the AD FS infrastructure and develop the appropriate claims rules for each target SaaS application, it's still necessary to determine how users will actually use SSO to access these applications. Most likely you will have to either create a portal where users can access these applications, or integrate access to them into the existing corporate portal.

Clearly AD FS 2.0 is a powerful platform that can be leveraged to integrate AD with SaaS applications; ultimately however, an organization must commit considerable time and money to achieve and maintain an end-to-end solution that really only addresses one-third of the Active Directory integration challenges.

Option 3: Use a Third-Party Vendor Solution

As the deployment of SaaS applications has accelerated, several vendors have emerged to help enterprises address their single sign-on and user management needs. To make a complete evaluation of any of these vendors, you must understand their ability to integrate with Active Directory. Unlike an application-specific integration strategy, these solutions provide a single point of integration with your on-premises Active Directory that can be federated across all of your SaaS applications. And unlike the AD FS option, some vendors also provide a complete solution that is maintained for you and works with your existing AD infrastructure.

When evaluating the AD integration these vendors offer, there are several factors to consider:

- Is it a solution or a toolkit? The right option should not require you to purchase additional products or pay for installation services, and it should not require custom development before users can start realizing the benefits. Instead it should provide:
  - Seamless integration with AD, with no services engagement required.
  - A large catalog of pre-integrated business and personal applications.
  - Integration with AD that addresses the previously mentioned key three requirements: two-way user and group synchronization, single sign-on, and provisioning/deprovisioning.
  - A portal that enables single sign-on for each user to access all of their SaaS applications.
  - Administrative tools that enable user, application, and AD integration management from one console, anywhere, anytime.
- Do I need to purchase and maintain hardware? The right solution, like the SaaS applications themselves, should be 100 percent on-demand, highly available, and require no hardware.
- Are the integrations maintained over time? A complete solution should also insulate your business from changes in the underlying SaaS applications and ensure that you can manage users and SSO over time.

- Is the integration secure and configuration-free? Any integration with AD should be outbound, and should take place over standard HTTPS to ensure security and avoid the need to make any changes to your existing firewall configuration.
- Will the architecture degrade user experience? To maximize performance and user experience, an SSO solution should authenticate a user and then get out of the way. Routing all traffic through a proxy creates bottlenecks, degrades performance, and typically does not scale as usage increases.

Okta: AD Integration for All Your SaaS Applications

Okta is an enterprise grade identity management service, built from the ground up in the cloud and delivered with an unwavering focus on customer success. The Okta service provides directory services, single sign-on, strong authentication, provisioning, workflow, and built in reporting. Enterprises everywhere use Okta to manage access across any application, person or device to increase security and productivity, and maintain compliance.

The Okta service features the industry's most unified, comprehensive, and easy-to-use Active Directory integration solution. The Okta service and Active Directory integration component provide:

- A complete end-to-end solution that requires no services to install and includes:
  - Self-configurable, secure, and fully automatic integration with your existing AD infrastructure, with no manual group mappings required.
  - A large catalog of preintegrated business and personal applications. Okta manages and updates the integrations so you never have to worry about continued seamless integration as underlying applications change.
  - A single sign-on home page and mobile application for every user that offers one-click access to all of their web applications.
  - An integrated administrative experience that allows you to manage users, applications, and your AD integration from one console, anywhere, anytime, and on multiple devices.
- Real-time synchronization. Securing your environment requires that terminated employees lose access immediately.
- Two-Way Sync. For hybrid environments with both on-premise and cloud services Okta enables SaaS applications to push groups and user profiles back to AD.
- A 100 percent on-demand offering. Okta's core service is a multi-tenant solution with a very light footprint and an AD agent that installs locally but without any appliances to buy or maintain.
- Seamless High Availability. Failover between Okta agents running in parallel is instantaneous and results in no interruption of service for your users, and requires no dedicated hardware.

- A single AD integration that enables you to configure once and then federate Active Directory across all of your SaaS applications.
- Outbound AD connection over HTTPS. Okta's lightweight agent makes a secure, outbound-only connection over HTTPS—no firewall configuration changes are required.
- Out- of-band authentication. Okta authenticates a user with the SaaS application and then gets out of the way. All ongoing traffic is between the user and the application.
- Integration with trusted and untrusted Active Directory domains in parallel.

Getting Started with Your Free Trial

To discover how easy it is to establish a comprehensive integration with Active Directory for your SaaS applications, and to begin securely scaling your cloud-based applications, visit www.okta.com/freetrial to get started with Okta.

About Okta

Okta is the foundation for secure connections between people and technology. By harnessing the power of the cloud, Okta allows people to access applications on any device at any time, while still enforcing strong security policies. It integrates directly with an organization's existing directories and identity systems, as well as 4,000+ applications. Because Okta runs on an integrated platform, organizations can implement the service quickly at large scale and low total cost. More than 2,500 customers, including Adobe, Allergan, Chiquita, LinkedIn, MGM Resorts International and Western Union, trust Okta to help their organizations work faster, boost revenue and stay secure.

For more information, visit us at www.okta.com or follow us on www.okta.com/blog.