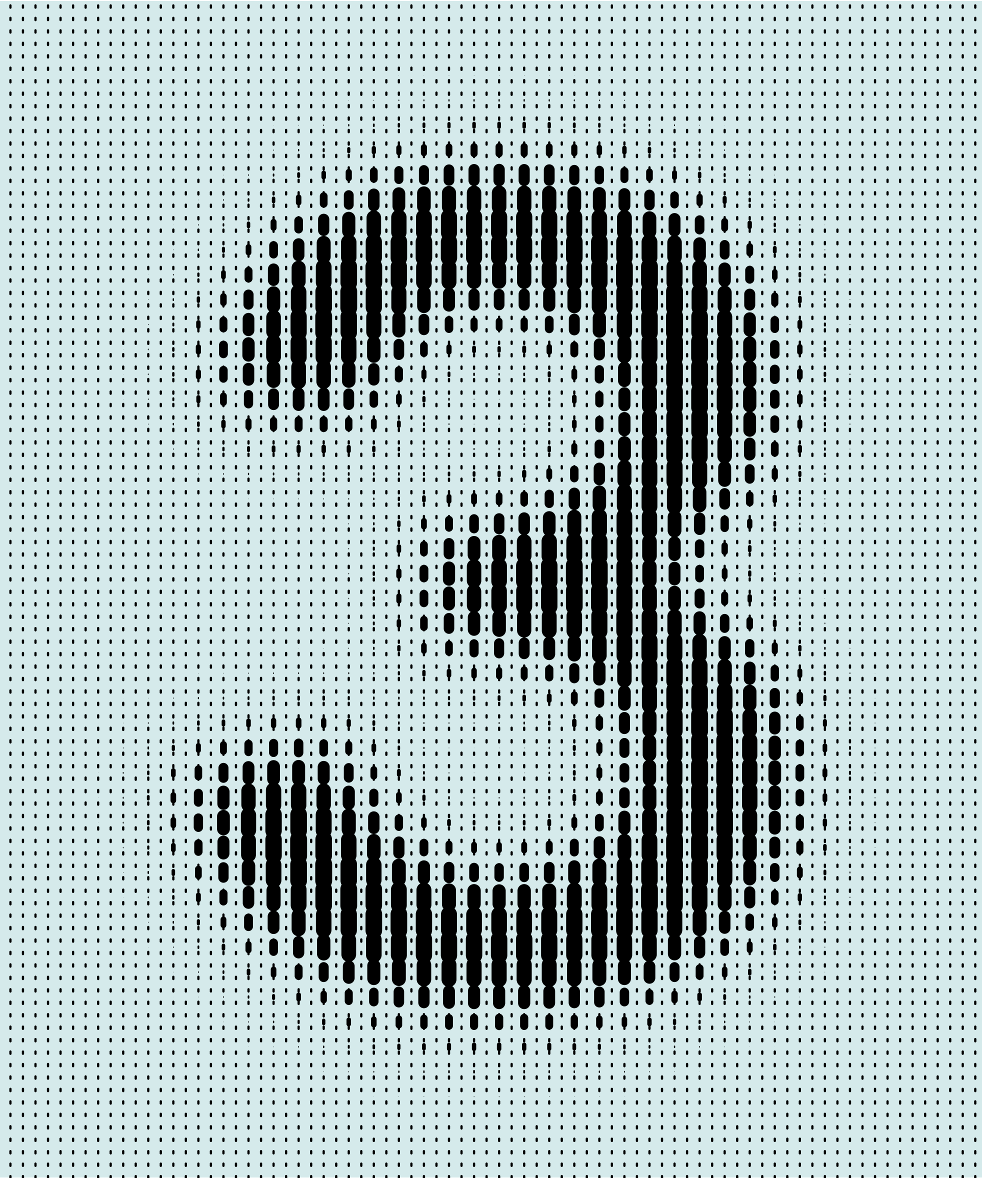
Whitepaper

January 2021

Three Ways to Integrate Active Directory with Your SaaS Applications

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871



Contents

Challenges of Software as a Service

The adoption rate of software as a service (SaaS) has been dramatic in recent years, moreso in 2020. In a recent **study**, 54 percent of IT and security leaders confirm that the COVID epidemic accelerated migration of user workflows to cloud-based apps. Trials of applications like Salesforce, AWS, and Workday have transitioned to enterprise-wide deployments, and many organizations have adopted “SaaS first” policies.

However SaaS adoption is not without its challenges. SaaS applications tend to be siloed, and that 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. This can introduce security risks. For example, because there is frequently no central user directory, oftentimes access is not revoked right away when an employee leaves the company, permitting the former employee to retain access to critical systems. And while Zero Trust has dismissed the idea of the trusted internal network, and has been a boon to productivity, it poses adoption challenges. IT departments must find a way to harness the benefits of SaaS, while minimizing business risk.

The Importance of Active Directory Integration

For years, in most enterprises, Microsoft Active Directory (AD) has been the authoritative user directory that governs access to basic IT services. But AD has proven to be a challenge to cloud adoption. SaaS applications have their own native user directories and often are not connected to Active Directory. This is because AD was used to control access to a broader set of business applications and IT systems. It was not designed to live in the cloud or easily integrate with cloud applications.

AD’s future is not guaranteed. And yet many companies are still using it today. Thus it’s critical for IT to find ways of seamlessly integrating their applications to AD. 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 cloud user directories in addition to Active Directory can easily lead to a set of untenable security and access management challenges. To help customers move to the cloud, 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 access 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 Workspace, Microsoft Azure AD, and Salesforce.com are all prominent examples of this approach. And all have notable issues.

Google Cloud Directory Sync provides one-way pushing of users from Active Directory into a Google Workspace 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 Suite 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 importantly, 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 Azure AD Connect also provides one-way pushing of users from Active Directory into Azure AD. Administrators can use this tool to both provision and deprovision users in Azure AD (Microsoft 365) when they are added or removed from Active Directory. Similar to the Google Workplace 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 created Identity Connect at additional licensing costs. The setup however is complex and siloed from the Salesforce administrative experience—you have to manage it on the local server. In addition, it only integrates with a single Salesforce org. Integrating with multiple Salesforce orgs requires additional servers and the costs associated with maintaining and licensing those servers.

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, and has continued to release AD FS on Windows Server 2019, 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 and deprovisioning.

But AD FS is a free solution, so why wouldn't organizations use it? As a feature of Windows Server, there are three server roles that make up AD FS itself—the Federation Service, the Federation Service Proxy, and the web server agent. When considering AD FS to address SSO needs, it's imperative to consider that AD FS–based solutions require both hardware and software.

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, in fact, 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. Once 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, 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 for Windows Server 2019 is a powerful feature set that can be leveraged to integrate AD with SaaS applications. However, an organization must ultimately 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. Not to mention in today's growing modern SaaS environment, adding additional on-prem hardware will not help organizations scale, it will only help them increase maintenance costs, slow speed of work, and increase their attack surface.

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-built integrations to business and personal applications.
    - Integration with AD that addresses the three previously mentioned key requirements: two-way user and group synchronization, single sign-on, and provisioning and 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 Customer First focus. The Okta service provides directory services, single sign-on, strong authentication with MFA, provisioning, customizable workflows, 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.

Okta 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.** Our AD integration 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 pre-integrated business and personal applications Okta manages and updates the integrations so you never have to worry 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-premises 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.** Configure it 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 aSaaS application and then gets out of the way. All ongoing traffic is between the user and the application.
- **Trusted and untrusted domain coverage.** Okta provides integration with trusted and untrusted Active Directory domains in parallel.

Get 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. To see how easy it is to set up, follow the QR code to watch a video (QR Code link to a video)

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 8,950 organizations, including JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers. Learn more at **www.okta.com**.