Cloud: This is everyone. Everyone: Meet Cloud.

Integrate Active Directory with your cloud app for hassle-free (and budget-free) SSO.

If you're like most organizations, you already have an infrastructure to manage employee identities. It's called Microsoft Active Directory (AD), and it serves as your employee database, allowing you to set up profiles and enforce authentication and access policies for all the applications you host on your own servers, within your company firewall.

But what happens when you decide to offer productivity, collaboration, or customer management tools in the cloud? Syncing AD user profiles with those in Google Apps, for example, is a manual process fraught with inefficiency and security risk. Every time someone changes jobs or leaves the company, IT has to update both AD and your cloud app. The hassle extends to employees, who struggle to manage multiple passwords—and to IT administrators, who spend countless hours holding people's hands as they reset those passwords.

Clearly a single sign-on (SSO) system that integrated AD with even just one cloud app would be tremendously valuable. That's how we came up with Okta Cloud Connect.

It's simple. Extend AD to the cloud application of your choice. For free.

Modern technology is awesome. Once you accomplish the sometimes complex work of getting two applications to work together, you can duplicate that integration in an almost infinite number of scenarios with very little effort.

So here's the deal: Okta developers have already integrated with a long list of common enterprise apps. Okta Cloud Connect offers you a chance to benefit from that work, with the enterprise cloud app of your choice. Connect to your AD using the Okta agent, and in a matter of minutes you can solve a multitude of login and user administration issues—for an unlimited time, for an unlimited number of people, free of charge.

Let's just say we're so sure your whole organization will love it that soon you'll want to SSO into more apps—and we'll be happy to charge you for those.

Delegated authentication. Desktop SSO.

Okta Cloud Connect makes it so your employees log in to your cloud app with the same AD or LDAP credentials they use to log into all their other applications. If they log in to your Windows domain from their desktops with Windows network credentials, that's even better. Okta's support for Integrated Windows Authentication allows you to make the SSO experience even more seamless.

Administration tasks: Cut in half.

Integrate your cloud application tightly with AD, and you cut user management tasks virtually in half. After Carla logs into her PC in the morning, she can access your enterprise cloud app without a log-in at any time. When she changes her AD password, her cloud app password changes immediately, as well. When she leaves the company, disable her profile from AD and you also disable her cloud access.

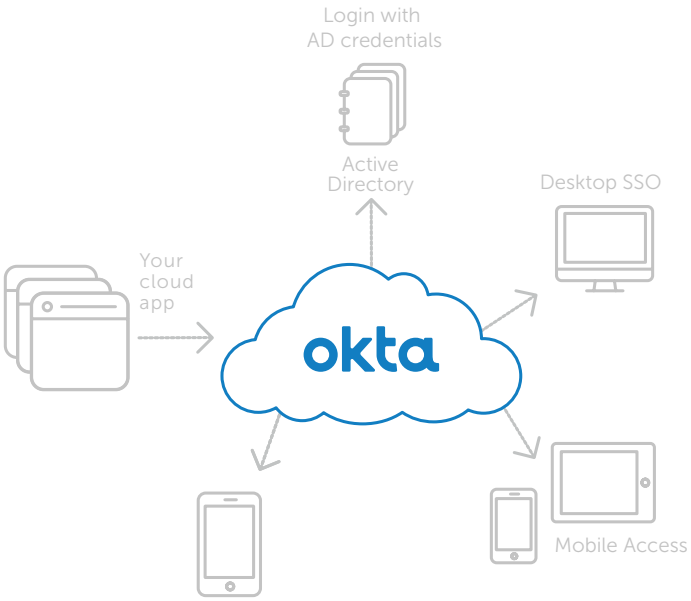
Set-up is simple.

1. Download the Okta agent and install it on any Windows Server that has access to a Domain Controller. No network or firewall configuration needed.
2. Configure single sign-on and provisioning settings for your cloud app.
3. Assign the app to a set of users, and set future assignment rules.

How does it work?

After you integrate AD with Okta, a simple configuration change in your cloud app console shifts the authentication process from the cloud app to Okta by way of Security Assertion Markup Language. Then, all user credentials are entered and verified via the Okta agent with your AD server. Neither Okta nor your cloud app provider stores any passwords. The AD server remains your single source for authentication.

Okta Cloud Connect integrates your cloud app with AD and your existing user lifecycle management around AD. Now, your cloud accounts are automatically provisioned according to AD users and security group membership. As changes happen in AD, Okta syncs them with your cloud app automatically, at configurable intervals, so that access privileges are always up to date. When you disable users in AD, their access to your cloud app is immediately revoked. Okta suspends the account to prevent access from any other clients or devices, as well.



What apps can I connect?

We continually add apps to Okta Cloud Connect. Please check www.Okta.com/free-forever for the most current list. Here are some of the most popular ones:

- Amazon Web Services
- Box
- DocuSign
- Dropbox
- GoogleApps
- Office365
- Salesforce
- ServiceNow
- Workday
- Zendesk
- Zscaler

How secure is it?

Communication between the Okta agent and Okta Cloud Connect for your particular cloud app is protected with SSL encryption. Server-side SSL certificates prevent man-in-the-middle attacks. The agent authenticates to the service by first using organization-specific credentials, then exchanging cryptographic keys used for all future communication. You can revoke an agent's access at any time by deactivating its security token.

Already using a pre-integrated, third-party multi-factor authentication solution such as YubiKey, RSA, or Symantec? You can enable it as well, for an extra layer of protection.

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 protections. 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.

Thousands of customers, including Adobe, Allergan, Chiquita, LinkedIn, and Western Union, trust Okta to help their organizations work faster, boost revenue, and stay secure.

www.okta.com