Extending Active Directory and LDAP to the Cloud

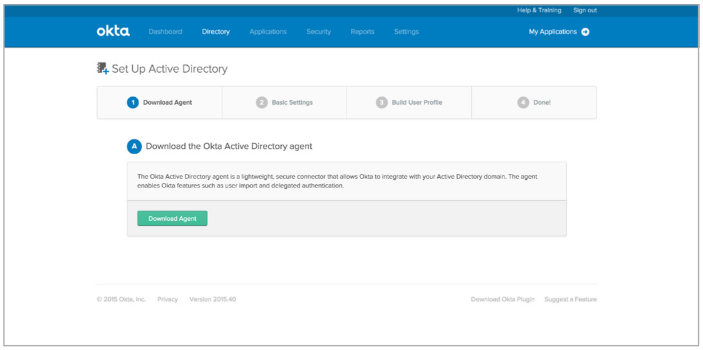
Teach your old directory service new tricks

Active Directory and the cloud

Microsoft Active Directory (AD) is central to many organizations' identity and access management policies. These policies regulate access to critical on-premises resources such as the network, file servers, applications, and other objects by connecting them to a unified user store. When Active Directory federates identity across these resources, and consolidates multiple user credentials into a single username and password, people become more productive. As apps and data shift to the cloud, it's crucial to extend AD to these resources so you can maintain data integrity while making sure your people don't miss a beat.

Single sign-on and user management for all your web applications

Okta's on-demand identity and access management service offers the most complete, most reliable and easiest-to-use Active Directory integration. With Okta, IT can extend AD to the cloud for single sign-on, automated provisioning, deprovisioning, and reporting across web-based applications, whether the apps are in the cloud or behind the firewall. Admins get a central place to control both cloud and on-premises applications, and your people can simply continue using their AD credentials to access all of it - as if they had a master key that fit all locks.



Set Up Active Directory

1 Download Agent · 2 Basic Settings · 3 Build User Profile · 4 Done!

A Download the Okta Active Directory agent

The Okta Active Directory agent is a lightweight, secure connector that allows Okta to integrate with your Active Directory domain. The agent enables Okta features such as user import and delegated authentication.

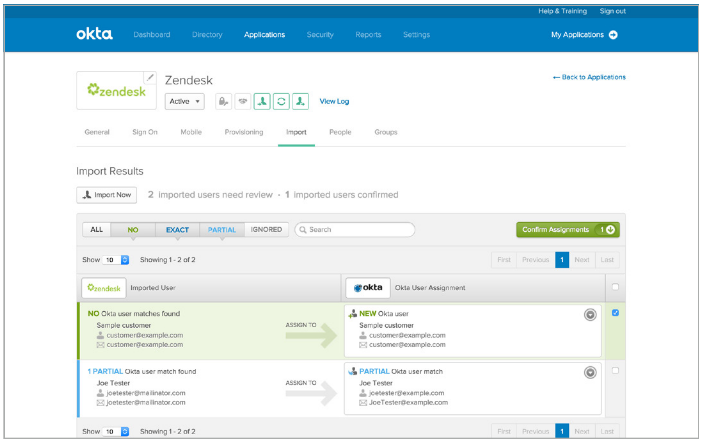
Set Up Active Directory

Easy to install and configure

Okta's AD integration is a simple, wizard-driven process. With a click of a button from the Okta admin portal, you can download the Okta Active Directory agent and install it on any Windows server that has access to a domain controller. Once installed, enter the URL of your company's Okta organization, along with your credentials, and the agent securely establishes a connection between AD and your Okta instance. No network or firewall configuration required.

A smart way to synchronize users

Once the agent is installed, and the initial user import takes place, Okta intelligently processes the results. Matching algorithms are applied to analyze the incoming AD users and determine if they correspond to existing Okta users. You can also apply the algorithms to accounts imported from other SaaS systems. Future user imports can be scheduled or performed on demand.



Import Results

Import Now 2 imported users need review · 1 imported users confirmed

Showing 1 - 2 of 2

zendesk Imported User		okta Okta User Assignment	□
NO Okta user matches found Sample customer customer@example.com customer@example.com	ASSIGN TO	NEW Okta user Sample customer customer@example.com customer@example.com	☑
1 PARTIAL Okta user match found Joe Tester joetester@mailinator.com joetester@mailinator.com	ASSIGN TO	PARTIAL Okta user match Joe Tester joetester@example.com JoeTester@example.com	□

Show 10 Showing 1 - 2 of 2

Intelligent user sychronization

Rule-based provisioning and deprovisioning

Okta can automatically provision applications to people based on AD security group membership and other rules. Here's how it works: Add a user to AD and place them in a security group. In Okta, map the application you want to provision to that security group. When AD is synchronized with Okta, accounts will automatically be provisioned in the application mapped to that security group. Even more importantly, when someone is disabled or deleted in Active Directory, Okta detects the change and deactivates the user from Okta and from any applications assigned to that user. Okta also provides a deprovisioning audit trail so administrators can demonstrate compliance across any cloud application by simply running a standard report.

Delegated authentication

People can log in to Okta with their AD credentials. With delegated authentication, Okta verifies a user credential through the agent with the AD server. No password is stored in the Okta service—the AD server remains the single source for authentication. For people who have already authenticated to the domain with their Windows network login, Okta leverages Integrated Windows Authentication (IWA) to provide true single sign-on.

High availability architecture

Okta's service supports multiple Okta AD agents running in your environment to provide higher throughput and redundancy and thus greater availability. If one of the agents stops running or loses network connectivity, the authentication requests are simply routed to the other agents.

Okta Active Directory Agents run on any domain member server. The minimal system requirements are:

- Windows Server 2003 R2 or later
- Domain Users permissions
- Access to the public Internet for outbound connections of TCP port 443 (SSL)

Secure integration

Security is a key component of the Okta Active Directory Agent. Communication between the agent and the Okta cloud service is protected with SSL encryption. Man-in-the-middle attacks are prevented using server-side SSL certificates. The agent authenticates to the service by first using organization-specific credentials, then exchanges cryptographic keys that are used for all future communication. Any agent's access can be revoked at any time by deactivating its security token.

Simple, scalable, always on.

Feature rich, reliable, and easy to administer, Okta provides the industry's best integration with Active Directory from the cloud. In a matter of minutes you can integrate your cloud applications with Active Directory; configure user synchronization, provisioning and deprovisioning; and enable your users to seamlessly use Active Directory to gain access into any cloud application managed by Okta.

Get started with a free trial

Come experience Okta for yourself. Try Okta for free today.

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.

okta.com