

RVP

REDMOND VENDOR PROFILE

Okta: Extending Active Directory into the Cloud

Q Why do companies need an on-demand identity and access management service?

A The adoption rate of cloud-based or Software-as-a-Service (SaaS) applications has been dramatic. Just a few years ago, small groups in your company started experimenting with applications like Salesforce.com, WebEx, or NetSuite, and those trials have now transitioned into enterprise-wide deployments that store critical information and power core business processes. This shift to the cloud has changed how companies think about their IT infrastructure, and what they must do to manage it.

Q What does Okta do?

A As an on-demand identity management (IAM) service, Okta brings all of a company's cloud and web applications together. Our customers can then easily address the challenges of securing and controlling users and access, simplify the adoption and scaling of these applications, and get insight on usage and utilization to ensure that companies are optimizing their cloud investments. Specifically, we integrate with Active Directory to provision and de-provision users automatically; it provides a single sign-on for users to access all of their apps; and streamlines the IAM process for IT. Okta lets IT departments deploy a vendor-agnostic approach to managing different identities across on-demand and on-premise applications in order to mitigate security risks.

Q How do you install and configure against Active Directory?

A Enabling AD integration is a simple, wizard driven process. With the click of a button from the Okta administrative 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 you simply enter your Okta URL and credentials and the agent securely establishes a connection with your Okta instance—no network or firewall configuration required.

Eric Berg
VP Products
Okta



Eric is a former Director of Product Management for Microsoft System Center

Q Do you do any type of user synchronization?

A 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 there is a match to existing Okta users or to accounts that you have imported from other SaaS systems. Future user imports can be scheduled or performed on-demand.

Q What kind of provisioning and de-provisioning does Okta support?

A Okta can automatically provision applications to users based on rules such as AD security group membership. Just add a user to AD, place them in a security group, and when synchronized with Okta that user will be added, and an account in the application mapped to that security group will be automatically provisioned. Even more importantly, when a user is deactivated or deleted in Active Directory, Okta detects that change and deactivates the user from Okta, and their assigned applications. Okta also provides a de-provisioning audit trail so administrators can demonstrate compliance across any cloud application by simply running a standard report.

Q It would make sense to have some type of delegated authentication and desktop single sign-on capability. Is that in your future?

A As a matter of fact, users can log in to Okta with their AD credentials now. With delegated authentication, Okta verifies user credentials 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 users who have already authenticated to the domain with their Windows network login, Okta leverages Integrated Windows Authentication (IWA) to provide true single sign-on.

FREE TRIAL: To see how easy Okta makes extending Active Directory to web-based applications, please visit:
<http://www.okta.com/freetrial>

