

Purpose-Built Active Directory Integration for Workday

Single sign-on and automated user management that is simple, scalable, and reliable



- C × A / C +	Okta - Workday: MyCompany HR	/app/workday/instance/0pa 😒 🔻 🕅 🕻 Google
🕒 🕐 🕐 🛞 🕼 🕼 akta-admin.com (https://mycompany.okta-admin.com/admin/app/workday/instance/0ea 🏠 🔻) 👫 Coogle http://workday/.MyCompany.Htt 🔰 +		
) okta		Welcome Stephen Lee Sign
sshboard People Applicatio	na Security Reports Settings	My Applications
ma Halp		
Workday WyCompany HR		workday
AGTIVE Deactivate		& 10 A
General Sign-On User Mana	pernent Import People	« Back to Applications View System Log »
User Management Setting	JS	EdB User Management
Solar indultigentiate octaining Solar indultigentiate octaining Solar indultigentiate Workday API credentials	j s	_
✓ Enable user management —	wo-integration@jointa	User Management User management allows you to import users from an application and enables any additional
C Ensbie user management Workday API credentials Api Username Api Password	ws-integration@jointa	User Management User management allows you to import users from an application and enables any additional integration features.
✓ Enable user management Workday API credentials Apl Username	wo-integration@jointa	User Management User management allows you to import spees from an application and anables any additional integration features. User Import User Import
C Ensbie user management Workday API credentials Api Username Api Password	vel megatongalaa 	User Management Liver canagement allow you be report users from an exploritor hauters and any other hauters Liver Import a surventiably enabled when you can be used and the output of the output What do I seter for my API credential? • A suscent that can assume the API

Workday SSO and User Management

)- C 🗙 🏚 🐨 http://myco	mpany.okta.com/admin/app/active_directory/intg/ *	Coogle
) okta		Welcome Bob Lahblah Sign o.
cple Applications Security Repo ne Directories Help	rts Settings	My Applications 🤤
Windows Server Active Director mycompany.com ACTIVE Deectwate	y (Microsoft)	View System Log
Settings Import Active Directory Settings		
Agent Monitors		Add Agent
WIN-DJEUNJD2QK1 Dead	nate WIN-DJEUNJ02QK2 Desctivate	WIN-DJEUNJD2QK3 Deachade
This agent is active and healthy.	This agent is active and healthy.	This agent is active and healthy.
Agent Configuration (applies to all agents)		
Active Directory domain		
mycompany.com	This is usually the DNS domain handled by	tory domain you would like the agent to import from, the domain controller. For example, if your VY, the namino controller that domain is most

Active Directory Homepage

The Growth of Workday in Your Organization

Workday is one of the most popular on-demand human capital management (HCM) applications. Workday's unified HR and Talent management solution provides services such as workforce lifecycle management, and employee benefit self-service that are used by every employee across all organizations - from HR administrators, managers to employees through self-service. With this growth comes the need to ensure users have seamless access via single sign-on (SSO) and that their Workday user records are created, updated, and deactivated on an integrated cycle with the rest of the systems in IT.

Active Directory & Workday

For many Workday customers, Microsoft Active Directory (AD) is a core piece of their identity management infrastructure. Serving as the enterprise directory, user authentication and application access policies around on-premise applications are often tied to users and security groups in AD. As an HCM system, Workday should be tightly integrated with AD to align the user information in the two systems. End users should be able to leverage their AD credentials when accessing Workday and have their AD profile and security group membership defined based on their Workday user record.

Without native AD integration, administrators must manually synchronize Workday user records with their AD profile starting with the initial user creation during the onboarding process. Any subsequent user profile changes, such as job title or department, require manual updates as well. When a user leaves the organization, his AD account might be disabled while his Workday account will still be active or vice versa - unless administrators manually deactivate the account in a timely manner. These manual processes are inefficient and extremely error-prone. The hassle extends to the end-users who now need to deal with yet another password stored in Workday. Users struggle to manage their passwords and administrators spend countless cycles managing password resets.

As a result, user productivity is impacted - and the risk of exposing inappropriate access increases.

Okta Cloud Connect for Workday

Okta is a 100-percent on-demand, turnkey solution that automates user management and SSO with cloud and web applications. Okta Cloud Connect for Workday offers a complete, robust, and easy-to-use AD integration with Workday to provide a seamless authentication experience for Workday users and automated provisioning and deprovisioning between Workday and Active Directory. Other benefits include:

OKTA DATASHEET: OKTA CLOUD CONNECT FOR OFFICE WORKDAY

- Automated and orchestrated provisioning workflow between Workday and Active Directory
- Users can log in to Workday with their AD credentials
- Organizations can use Integrated Windows Authentication (IWA) for true SSO with Windows domain
- Automated Workday account deactivation is triggered directly from AD

Easy to install & Configure

Okta's Cloud Connect for Workday is a purpose-built solution targeted at seamlessly integrating Workday with Active Directory. With the click of a button, you can download the Okta Active Directory agent and install it on any Windows Server that has access to a Domain Controller. No network or firewall configuration required.

Enabling automated user management for Workday is equally simple. Through the Workday User Management configuration in Okta, integration can be done in minutes to enable account provisioning, profile updates, and account deprovisioning between AD and a Workday instance.

Delegated Authentication & Desktop SSO

With the AD integration completed, a simple configuration change in the Workday SSO setup console enables delegated authentication with Okta. Users can now log in to Workday with their AD credentials. With delegated authentication, Workday verifies user credentials through Okta and the Okta Active Directory agent with the AD server. No password is stored in Workday or Okta - the AD server remains the single source for authentication. No need to remember another password or reset your Workday password. Your AD password is your Workday password. For users who have already authenticated to the Windows domain with their Windows network login, Okta's support for IWA provides a true single sign-on experience to your Workday account.

Automated User Management

Okta Cloud Connect for Workday integrates Workday with Active Directory and your existing user lifecycle management around AD. Workday accounts can be automatically provisioned based on AD users and security group membership. If Workday is your authoritative source of user records, then AD account creation can be triggered from Workday. As changes are made in Workday and AD, Okta ensures that synchronization between AD and Workday occurs automatically at configurable intervals to ensure that access privileges are always up-to-date. With Workday authenticating users directly against AD, when a user is disabled in AD, his access into Workday is immediately revoked. Furthermore, Okta will set the Workday account status to inactive - ensuring proper account deactivation within Workday.



Integrating AD with Workday

Secure Integration

Security is a key component of the Okta Active Directory Agent. Communication between the agent and Okta Cloud Connect for Workday 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 exchanging cryptographic keys used for all future communication. Further, any agent's access can be revoked at any time from the service by deactivating its security token.

About Okta

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 are using Okta to manage access across any application, person or device to increase security, make people more productive, and maintain compliance.

The hundreds of enterprises, thousands of cloud application vendors and millions of people using Okta today also form the foundation for the industry's fastest growing, vendor neutral Enterprise Identity Network.

The Okta team has built and deployed many of the world's leading on-demand and enterprise software solutions from companies including Salesforce.com, PeopleSoft, Microsoft, BMC, Arcsight, Sun, and HP. Okta is backed by premiere venture investors Andreessen Horowitz, Greylock Partners, Khosla Ventures and Sequoia Capital.

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

