Automated Access + Provisioning— Informed by Workday, Enforced by Okta

Introducing a common ground for HR and IT to manage the employee lifecycle

Workday is one of the most popular providers of on-demand human capital management applications, offering companies like Avon, Bank of America and Hewlett-Packard the ability to manage everything from health insurance and health savings accounts to retirement savings and flex plans with a single unified system.

Large enterprises rely on Workday as an authoritative source of information about their people. Every stage of an employee's experience, beginning with their pre-hire interactions and start date and continuing through to his or her transfer and termination is managed by Workday. Meanwhile, the same user lifecycle is managed by IT as the systems and data that an employee has (or doesn't have) access to must be adjusted to reflect changes in her role. These dual relationships create the need for a closely coupled and automated identity lifecycle management solution.

Disconnected systems force manual processes

HR and IT serve the same set of stakeholders: employees. Yet for many Workday customers, a great disconnect exists between their HR apps and IT systems. In many cases, there is no direct integration between Workday and Microsoft Active Directory (AD) or with applications like email, web conferencing and other critical business applications. Without this integration, automation becomes impossible. IT administrators often rely on file dumps from Workday to provision or de-provision users from other systems. They end up manually synchronizing Workday user records with AD

and with essential business applications as people's roles change or when they leave the organization. With thousands of people in an organization, these manual updates can take a toll on productivity. Inefficient and error-prone, they can also create a security risk.

Automating the identity lifecycle with Workday and Okta

Active Directory is central to identity management for most companies. User authentication and application access policies are tied to users and security groups in AD. If HR systems like Workday are tightly integrated with AD, then user information can be automatically aligned. A person can access Workday with AD credentials and have his or her AD user profiles and security group memberships defined by Workday user records (and vice versa).

Okta's cloud-based identity management service offers the easiest way to integrate Workday with IT systems like Active Directory and other critical business applications. With Okta, multiple user credentials can be replaced with a single, Workday-driven identity. Any changes made to a user profile in Workday are automatically communicated back to Okta and are then applied to AD and any other apps that the company uses. New apps, whether they are on-premises, in the cloud, or on mobile devices, can be added quickly and securely.

Employees get access to the apps they need on any device or browser, while IT frees up valuable resources by automating processes that used to be manual.

Why use Okta?

- Automated provisioning and deprovisioning of users driven by Workday

- Automated AD account creation and deactivation driven by Workday

- Automated AD password management

- Scheduled synchronization (hourly, daily, or on-demand)

- Single Sign-on for Workday and all other applications on all devices

- Adaptive Multifactor Authentication

- Centralized reporting and audit of user access across all apps and systems

Easy to install and configure

Connecting Workday to Okta is extremely simple. Integration can be done in minutes. Just configure the Workday application in Okta, establish Workday as an import target, and set up single sign-on. The last step will allow seamless access into Workday once a user is created in Okta.

Integrating Workday to AD

Okta's AD integration can be set up with just a few clicks. First, download the Okta Active Directory agent from the Okta administrative portal. Next, install the agent on any Windows server that has access to a Domain Controller. No network or firewall configuration is required. Okta maps Workday employee attributes to Active Directory attributes, while a simple configuration change in the Okta AD setup turns on the automated provisioning of Active Directory accounts from Workday.

With Okta, companies conserve their IT resources. Starting from day one, Okta will manage the entire provisioning workflow—including scheduled imports from Workday, AD account creation, temporary password generation and notifications for new users. New employees will be able

to get up and running on their own, and existing employees will have instant access to applications that leverage AD as a user store. They will also be able to use approved web apps.

Single sign-on

Okta gives users access to enterprise apps in the cloud, on premises, and on mobile devices via a single set of credentials. Single sign-on is supported by the Okta Application Network, which offers the industry's broadest catalog of out-of-the-box integrations.

For companies seeking to synchronize user information in Workday and Active Directory, AD becomes the single source of authentication. Users log in to Okta with their AD credentials to get access to Workday, or, if they are on a PC or a Mac, they can just log in to Windows with their network login. Companies who want to further secure Workday or other apps can turn on adaptive multifactor authentication. With Okta, users can verify themselves with a comprehensive set of factors ranging from SMS to Voice, Push, Okta Verify OTP factors and 3rd party MFA providers.

A committed partnership

Okta's integration with Workday is a joint development effort that is marked by continuous improvement. The two companies have a strong, comprehensive partnership that spans executive management, research and development, and sales and services. Together, Okta and Workday introduced features such as Workday Provisioning Groups in Workday and enhanced provisioning workflows in Okta. Workday and Workday SI Partners work closely with Okta during new deployments to ensure customers are successful.