SailPoint + Workday:
Go Beyond Day 1
Access and Compliance

The success of an organization is highly dependent on the satisfaction of its employees. Employee satisfaction comes not only in ensuring they have access to an HR Cloud-based solution, such as Workday, to give them a strong start and drive continual employee engagement, but also ensuring they have timely access to the applications, systems and data necessary to perform their job.

However, the process of requesting and fulfilling approved access can be a challenging one. Many companies are using manual processes to handle these tasks which are time consuming and result in loss of user productivity and security risks. Some have turned to access management or single-sign on solutions which authenticate user's access to your network and applications. While this is a step in the right direction, organizations are finding it's not enough. To truly ensure access is authorized and aligns with security and compliance programs, they turn to identity governance. Identity governance goes beyond access management and focuses on granting and controlling access based on compliance-based policies – ensuring that users are authorized to only see and touch information within applications and file folders that are relevant to their job.

Integrating SailPoint cloud identity governance with Workday enables organizations to ensure user access is compliant starting day 1. By utilizing access policies to automatically determine and control who gets access to what, organizations can ensure data privacy and compliance requirements are adhered to throughout a user's tenure at the organization.

How it Works

SailPoint's connectivity to Workday enables organizations to leverage Workday as a single source of truth for core identity governance tasks beginning with provisioning access for day 1. When changes are made within Workday, such as role changes or terminations, they sync with SailPoint and access is automatically adjusted through the rest of the ecosystem. In addition, pre-defined policies, such as separation of

duties, helps prevent toxic access combinations which can lead to fraud and theft of information. All access activity is then documented across the organization and provides compliance auditors the necessary information needed to demonstrate and prove compliance.
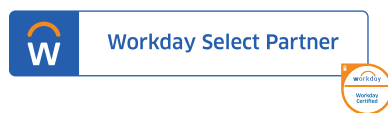
By integrating SailPoint with Workday, organizations can benefit in the following ways:
- **Day 1 Productivity** – new hire account creation is automatically provisioned
- **Least Privilege** – as user's roles are changed within Workday, access is proactively adjusted
- **Consistency** – account attribute changes such as last name, email address, etc. are automatically synced with other applications and systems
- **A Secure 'Good-bye'** – terminated employees, contractors and vendors automatically have their access deprovisioned in minutes not days or months
- **Confidence in Compliance** – since everything is documented by the system, it's easy to demonstrate access policy compliance to auditors

Additionally, by leveraging innovative AI and machine learning, organizations can proactively identify risky users and behavior, allowing them to start getting ahead of the ever-changing security curve.

SailPoint provides organizations complete visibility, control, and automation to ensure user access is authorized, entitlements are appropriate for their current job/role and access is frequently reviewed and certified to maintain a secure and compliant infrastructure.

As a Workday Select Partner with a certified Integration, SailPoint is the trusted cloud identity governance solution to automate, simplify and certify access for onboarding, offboarding and everything in between.

Workday Select Partner