March 2018

Understanding Workday security

Contact information
Juan Lopez
Workday consultant

Alight Solutions
workday.solutions@alight.com

Overview

Providing Workday access to a group of employees is a relatively simple task. Typically, all that's required is the creation of a security group and role, which is then associated with an organization (company, location, etc.) and assigned to a worker. However, granting access to an entire organization may be less than ideal, as specific individuals or sub-sets of groups may need to be excluded. This area is often overlooked during initial implementations, only to be revisited after deployment. Fortunately, Workday provides several solutions and tools to help with securing your data at a more granular level.

Architecting a smart security solution is easier than it sounds. It begins by asking basic questions: who, what, when, where and why?

Who: Security group

Who needs to have access? This is typically defined in Workday as a security group. The most common type is a role-based security group, wherein access is granted directly to a user, who becomes part of the group. It is commonly constrained to an organization (company, location, etc.). Security groups can also be unconstrained—thus, granting access across the entire system.

Security group: HR partner

— **Security group type**
Role-based security group (constrained)

— **Role use**
Supervisory organization, company, location

— **Access rights to organizations**
Applies to current organization and unassigned subordinates

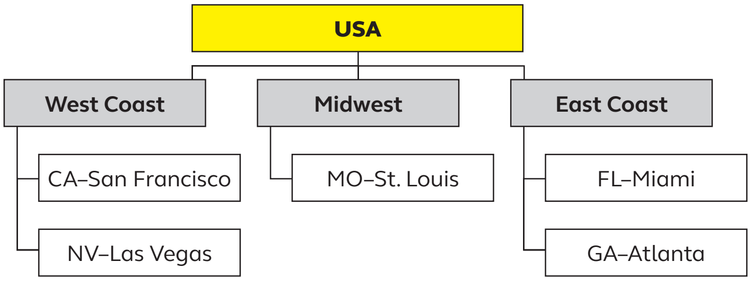
What: Domain

What are we securing? Workday secures data for functional areas at a domain level. The following is a sample set of domains within the functional area of core compensation. Each of these domains may hold different groups, allowing for dynamic security across the entire functional area.

Functional area: Core compensation

- Add compensation plans
- Compensation change
- Process: compensation plan employee
- Worker data: compensation
- Audit: compensation overall
- Self-service compensation
- Request: one-time payment
- Set up: base and plan
- Worker data: market position details
- Worker data: compensation plan type
- Worker data: total compensation
- Non-worker: compensation data by organization

Location hierarchy



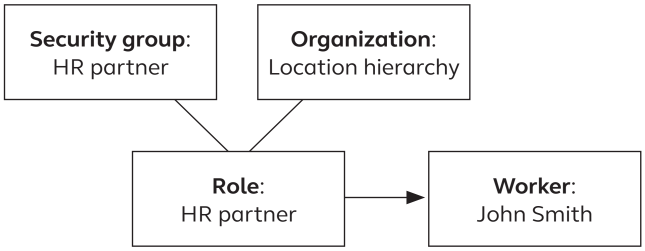
Where: Organizations

Where are we securing this data? Workday uses various organization types to secure data. The most commonly used groups are supervisory organizations, companies and locations. Workday also takes advantage of its strong organizational hierarchies to allow data access to flow, such as in the location hierarchy.

When: Role assignment

When do we assign security? Typically, security assignments are done with the utilization of a role. You must first create a role assignment, which ties your security group to your organization. Once the role has been configured, you may then assign it to specific workers at specific organizations, thus tying your configuration together.

Location hierarchy


Security group: HR partner
Organization: Location hierarchy
Role: HR partner
Worker: John Smith

Why: The business case

Why do we need this access? Whenever you are considering granting access within any system, it is important to understand why you're doing so. Also, are you sure you're not creating something that already exists? Security groups can exist across multiple domains, so it's important to make sure you're not creating groups merely for the sake of creating groups. You don't want to clog up your system with unnecessary security groups and assignments, as this can lead to challenges with performance and audits. Maintaining a clean and easy trail will help you manage issues, perform audits and ensure the long-term health of your system. Additionally, Workday delivers a large number of pre-configured roles, which are typically reviewed and configured during a Workday implementation. Leveraging these existing groups is always preferable to creating new security groups.

Once you have a good understanding of these five basic questions, you can begin configuring your solution.

Architecting a smart solution

When the time comes to bring your solution together, you must ensure you're testing the configuration of your solution within a Sandbox or Implementation environment and applying Workday's deployment methodology. Refer to this article in Workday community for more information.

Once you have configured your security group and roles, go to each domain where the security group will be granted access and update the level of access. Lastly, assign the roles to your workers and specify to which organizations they are allowed to have access. When it comes to security, you can never test enough, so be sure to check reports, user profiles and business processes to ensure access is appropriate based on your design.

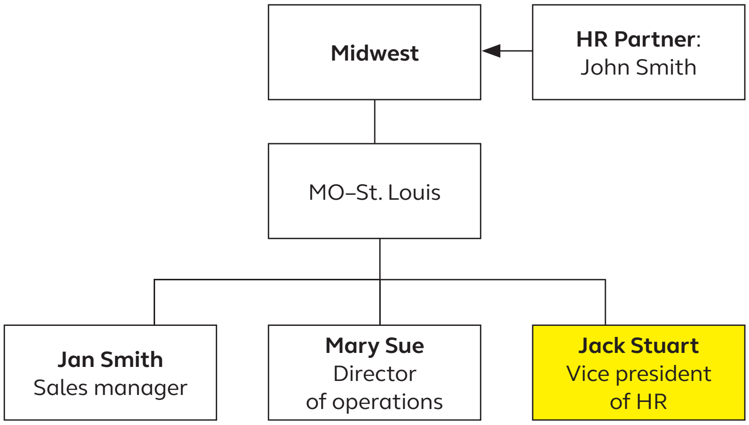
Securing your data further

Consider a scenario in which a standard security group isn't sufficient. An HR partner role was configured to be constrained by location. However this location houses an HR employee the HR Partner should not be able to access. To ensure this data is secure, we'll need to build a special security group which will exclude access to the Human Resources organization for all HR partners.

Intersection security group

An intersection security group uses two security groups or a security group and an organization to restrict access. In the previous scenario, we can use an intersection security group to help secure HR workers. This is accomplished by building an intersection security group that includes the security group "HR partner" and excludes the supervisory organization for "Human Resources."

Location hierarchy HR partner assignment



Security group: HR partner (no HR)

Security group type: Intersection security group

Included criteria: Security groups

- Security group: HR partner
- Security group type: role-based security group (constrained)
- Role use: supervisory organization, company, location
- Access rights to organizations: applies to current organization and unassigned

Excluded criteria: Supervisory organization

- Supervisory organization: human resources (applies to current organization and all subordinates)

Once this intersection security group has been created, we can update our domain's security policy to use this group instead of the "HR partner." This will limit the HR partner's access to both their existing assignment and exclude members of the Human Resources supervisory organization.

About Alight Solutions

As the leading provider of benefits administration and cloud-based HR and financial solutions, we enhance work and life through our service, technology and data. Our dedicated colleagues across 14 global centers deliver an unrivaled consumer experience for our clients and their people. We are Alight. Reimagining how people and organizations thrive.

alight.com

Alight: Your Workday security partner

When designing and executing Workday security changes, a strong partner is an essential component for success. Our Workday experts stand ready to guide you through every aspect of the process:

- **Advanced configurations**: Setting up segmented, intersection or custom security can pose challenges. We leverage our extensive experience deploying advanced configurations to simplify the project with a best-in-class approach.
- **Security assessments**: Our Workday experts review and assess your security configuration to identify redundancies, vulnerabilities, unassigned roles, deprecated functionality and critical configuration errors.
- **Audit reports**: Organizations often struggle to determine which Workday audit is most appropriate for managing their security model. Our custom reports empower you to hone in and review your organization's configuration to help maintain control of your security.
- **Workday updates**: At Alight, we would work with you to review your Workday security during the two annual updates. Our experts will also assist with the necessary configuration and set-up related to the new features that are often introduced during these updates, which can affect your security.
- **Strong point of view**: Whether you're designing a new configuration or revisiting an old one, you must consider the potential impacts across all of your modules. Leverage our expertise to help close the gap between Workday's various touch points to understand how it all comes together.
- **Design, execution and commitment to excellence**: Our certified Workday professionals are some of the best minds across all of Workday's functional areas. They bring extensive experience and know-how to assess and support your various projects and security needs.

Contact Information

For questions, contact workday.solutions@alight.com.